ADSL Router Series

P-660HNU-Fx, P-660HN-Fx, P-661HNU-Fx (x stands for 1 or 3)

User's Guide

Default Login Details

IP Address	https://192.168.1.1
Admin	User Name: admin Password: 1234
User	User Name: user Password: 1234

Firmware Version 3.10
Edition 1, 12/2011

ZyXEL

www.zyxel.com

Copyright © 2011
ZyXEL Communications Corporation

Videos

File Sharing Video Example 55
QoS Video Example 76

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator.

This guide is a reference for a series of products. Therefore some features or options in this guide may not be available in your product.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

- Support Disc

  Refer to the included CD for support documents.

Documentation Feedback

Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.

Need More Help?

More help is available at www.zyxel.com.



- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

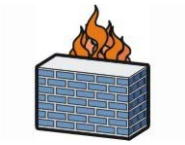
Syntax Conventions

- The P-66xHNU-Fx Series may be referred to as the "ZyXEL Device", the "device", the "system" or the "product" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

ZyXEL Device	Computer	Notebook computer
		

Server 	Firewall 	Router 
Switch 		

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- This CPE product is for indoor use only (utilisation intérieure exclusivement).

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



Contents Overview

User's Guide 19

Introduction 21
Introducing the Web Configurator 27
Tutorials 41

Technical Reference 81

Connection Status and System Info Screens 83
Broadband 87
Wireless 105
Home Networking 131
Routing 157
DNS Route 161
Quality of Service (QoS) 165
Network Address Translation (NAT) 175
Dynamic DNS 183
Firewall 185
MAC Filter 191
Certificates 193
VPN 203
System Monitor 223
User Account 227
Remote MGMT 229
System 231
Time Setting 233
Log Setting 235
Firmware Upgrade 237
Backup/Restore 239
Diagnostic 243
Troubleshooting 247
Product Specifications 255

Table of Contents

About This User's Guide 3

Document Conventions 5

Safety Warnings 7

Contents Overview 9

Table of Contents 11

Part I: User's Guide 19

Chapter 1
Introduction 21

1.1 Overview 21
1.2 Applications for the ZyXEL Device 21
1.2.1 Internet Access 21
1.2.2 Wireless Connection 22
1.2.3 ZyXEL Device's USB and Print Server Support 22
1.3 The WPS/WLAN Button 23
1.4 Ways to Manage the ZyXEL Device 24
1.5 Good Habits for Managing the ZyXEL Device 25
1.6 The RESET Button 25

Chapter 2
Introducing the Web Configurator 27

2.1 Overview 27
2.1.1 Accessing the Web Configurator 27
2.2 The Web Configurator Layout 29
2.2.1 Title Bar 29
2.2.2 Main Window 30
2.2.3 Navigation Panel 30
2.3 User Mode 32
2.3.1 Overview 32
2.3.2 What You Can Do 32
2.3.3 Navigation Panel 33
2.3.4 Network Map 33
2.3.5 Control Panel 34
2.3.6 Power Saving 34

2.3.7 Content Filter 35
2.3.8 Firewall 36
2.3.9 Wireless Security 37
2.3.10 WPS 38
2.3.11 Media Server 38

Chapter 3
Tutorials 41

3.1 Overview 41
3.2 Setting Up Your DSL Connection 41
3.3 How to Set up a Wireless Network 44
3.3.1 Example Parameters 44
3.3.2 Configuring the ADSL Device 44
3.3.3 Connecting Wirelessly to your ADSL Device 46
3.3.4 Configuring the Wireless Client using the WPS PIN number 48
3.4 Setting Up NAT Port Forwarding to Allow Access to Network Servers from the Internet 49
3.5 Using the File Sharing Feature 50
3.5.1 Set Up File Sharing 51
3.5.2 Access Your Shared Files From a Computer 54
3.6 Using the Print Server Feature 56
3.7 Configuring the MAC Address Filter for Restricting Wireless Internet Access 70
3.8 Configuring Static Route for Routing to Another Network 71
3.9 Configuring QoS Queue and Class Setup 73
3.10 Access the ADSL Device Using DDNS 77
3.10.1 Registering a DDNS Account on www.dyndns.org 78
3.10.2 Configuring DDNS on Your ADSL Device 78
3.10.3 Testing the DDNS Setting 79

Part II: Technical Reference 81

Chapter 4
Connection Status and System Info Screens 83

4.1 Overview 83
4.2 The Connection Status Screen 83
4.3 The System Info Screen 84

Chapter 5
Broadband 87

5.1 Overview 87
5.1.1 What You Can Do in this Chapter 87
5.1.2 What You Need to Know 87

5.1.3 Before You Begin 88
5.2 The Broadband Screen 88
5.2.1 Add/Edit Internet Connection 89
5.3 Technical Reference 100

Chapter 6
Wireless 105

6.1 Overview 105
6.1.1 What You Can Do in this Chapter 105
6.1.2 Wireless Network Overview 105
6.1.3 Before You Begin 107
6.2 The Wireless General Screen 107
6.2.1 No Security 109
6.2.2 Basic (Static WEP/Shared WEP Encryption) 109
6.2.3 More Secure (WPA(2)-PSK) 111
6.2.4 WPA(2) Authentication 112
6.3 The More AP Screen 113
6.3.1 Edit More AP 114
6.4 The WPS Screen 115
6.5 The WMM Screen 117
6.6 Scheduling Screen 118
6.7 Technical Reference 119
6.7.1 Additional Wireless Terms 119
6.7.2 Wireless Security Overview 119
6.7.3 Signal Problems 122
6.7.4 BSS 122
6.7.5 MBSSID 122
6.7.6 WiFi Protected Setup (WPS) 123

Chapter 7
Home Networking 131

7.1 Overview 131
7.1.1 What You Can Do in this Chapter 131
7.1.2 What You Need To Know 131
7.2 The LAN Setup Screen 134
7.3 The Static DHCP Screen 136
7.3.1 Before You Begin 136
7.4 The UPnP Screen 137
7.5 The File Sharing Screen 138
7.5.1 Before You Begin 139
7.5.2 Add/Edit File Sharing 140
7.5.3 Add New User 141
7.6 The Media Server Screen 142

7.6.1 The Media Server Screen 142
7.7 The Print Server Screen 143
7.7.1 Before You Begin 143
7.8 Technical Reference 144
7.9 Installing UPnP in Windows Example 148
7.10 Using UPnP in Windows XP Example 151

Chapter 8
Routing 157

8.1 Overview 157
8.2 Configuring Static Route 157
8.2.1 Add/Edit Static Route 158

Chapter 9
DNS Route 161

9.1 Overview 161
9.1.1 What You Can Do in this Chapter 161
9.2 The DNS Route Screen 162
9.2.1 Add/Edit DNS Route Edit 162

Chapter 10
Quality of Service (QoS) 165

10.1 Overview 165
10.1.1 What You Can Do in this Chapter 165
10.1.2 What You Need to Know 165
10.2 The QoS General Screen 166
10.3 The Queue Setup Screen 167
10.3.1 Add/Edit a QoS Queue 168
10.4 The Class Setup Screen 169
10.4.1 Add/Edit QoS Class 170
10.5 The QoS Monitor Screen 173
10.6 QoS Technical Reference 173
10.6.1 IP Precedence 174
10.6.2 DiffServ 174

Chapter 11
Network Address Translation (NAT) 175

11.1 Overview 175
11.1.1 What You Can Do in this Chapter 175
11.1.2 What You Need To Know 175
11.2 The Port Forwarding Screen 176
11.2.1 The Port Forwarding Screen 177
11.2.2 The Port Forwarding Edit Screen 177

11.3 The Sessions Screen 178
11.4 The ALG Screen 179
11.5 Technical Reference 180
11.5.1 NAT Definitions 180
11.5.2 What NAT Does 180
11.5.3 How NAT Works 180

Chapter 12
Dynamic DNS 183

12.1 Overview 183
12.1.1 What You Need To Know 183
12.2 The Dynamic DNS Screen 183

Chapter 13
Firewall 185

13.1 Overview 185
13.1.1 What You Can Do in this Chapter 185
13.1.2 What You Need to Know 185
13.2 The General Screen 186
13.3 The Services Screen 187
13.4 Firewall Technical Reference 188
13.4.1 Guidelines For Enhancing Security With Your Firewall 188
13.4.2 Security Considerations 188

Chapter 14
MAC Filter 191

14.1 Overview 191
14.1.1 What You Need to Know 191
14.2 The MAC Filter Screen 191

Chapter 15
Certificates 193

15.1 Overview 193
15.1.1 What You Can Do in this Chapter 193
15.1.2 What You Need to Know 193
15.1.3 Verifying a Certificate 195
15.2 Local Certificates 196
15.2.1 Trusted CAs 197
15.2.2 Trusted CA Import 198
15.2.3 View Certificate 198
15.3 VPN Certificates 199
15.3.1 Import Certificate 200

Chapter 16
VPN 203

16.1 Overview 203
16.1.1 What You Can Do in the VPN Screens 203
16.1.2 What You Need to Know About IPSec VPN 203
16.1.3 Before You Begin 205
16.2 VPN Setup Screen 205
16.3 The VPN Edit Screen 206
16.4 Configuring Advanced Settings 210
16.5 Viewing SA Monitor 212
16.6 IPSec VPN Technical Reference 212
16.6.1 IPSec Architecture 212
16.6.2 IPSec and NAT 213
16.6.3 VPN, NAT, and NAT Traversal 214
16.6.4 Encapsulation 215
16.6.5 IKE Phases 216
16.6.6 Negotiation Mode 217
16.6.7 Remote DNS Server 217
16.6.8 ID Type and Content 218
16.6.9 Pre-Shared Key 219
16.6.10 Diffie-Hellman (DH) Key Groups 219
16.6.11 Telecommuter VPN/IPSec Examples 219

Chapter 17
System Monitor 223

17.1 Overview 223
17.1.1 What You Can Do in this Chapter 223
17.2 The WAN Status Screen 223
17.3 The LAN Status Screen 224
17.4 The NAT Status Screen 225

Chapter 18
User Account 227

18.1 Overview 227
18.2 The User Account Screen 227

Chapter 19
Remote MGMT 229

19.1 Overview 229
19.1.1 What You Need to Know 229
19.2 The Remote MGMT Screen 229

Chapter 20
System 231

20.1 Overview 231
20.1.1 What You Need to Know 231
20.2 The System Screen 231

Chapter 21
Time Setting 233

21.1 Overview 233
21.2 The Time Setting Screen 233

Chapter 22
Log Setting 235

22.1 Overview 235
22.2 The Log Setting Screen 235

Chapter 23
Firmware Upgrade 237

23.1 Overview 237
23.2 The Firmware Screen 237

Chapter 24
Backup/Restore 239

24.1 Overview 239
24.2 The Backup/Restore Screen 239
24.3 The Reboot Screen 241

Chapter 25
Diagnostic 243

25.1 Overview 243
25.1.1 What You Can Do in this Chapter 243
25.2 The Ping Screen 243
25.3 The DSL Line Screen 244

Chapter 26
Troubleshooting 247

26.1 Overview 247
26.2 Power, Hardware Connections, and LEDs 247
26.3 ZyXEL Device Access and Login 248
26.4 Internet Access 250
26.5 Wireless Internet Access 251
26.6 USB Device Connection 252
26.7 UPnP 253

Chapter 27
Product Specifications 255

Appendix A IP Addresses and Subnetting 263

Appendix B Setting Up Your Computer's IP Address 273

Appendix C Pop-up Windows, Java Script and Java Permissions 303

Appendix D Wireless LANs 311

Appendix E Common Services 331

Appendix F Open Software Announcements 335

Appendix G Legal Information 357

Index 361

PART I
User's Guide

1

Introduction

1.1 Overview

The ADSL Router Series includes the P-660HNU-Fx, P-660HN-Fx, P-661HNU-Fx (x stands for 1 or 3). The routers in this series are ADSL2+ 4-Port Security Gateways with rich features and performance that use 802.11N technology to maximize the speed and range of your wireless signal. The ZyXEL Device is also a complete security solution with a robust firewall based on Stateful Packet Inspection (SPI) and Denial of Service (DoS) protection.

Please refer to the following description of the product name format.

- "H" denotes an integrated 4-port hub (switch).
- "N" denotes wireless functionality, including 802.11n mode. There is an embedded mini-PCI module for IEEE 802.11 a/b/g/n wireless LAN connectivity.
- "U" denotes a USB port used to share files via a USB memory stick or a USB hard drive. The ZyXEL Device can function as a print server with a USB printer connected.
- Models ending in "1", for example P-661HNU-F1, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in "3" denote a device that works over ISDN (Integrated Services Digital Network) or T-ISDN (UR-2).

Only use firmware for your ZyXEL Device's specific model. Refer to the label on the bottom of your ZyXEL Device.

See the chapter on product specifications for a full list of features.

1.2 Applications for the ZyXEL Device

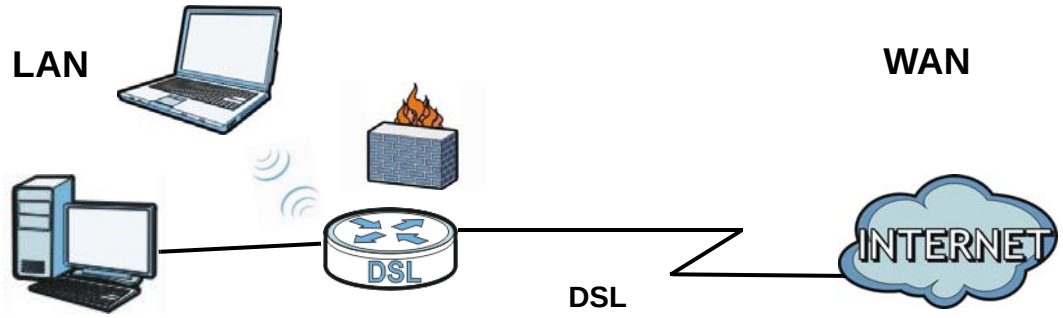
Here are some example uses for which the ZyXEL Device is well suited.

1.2.1 Internet Access

Your ZyXEL Device provides shared Internet access by connecting the DSL port to the **DSL**/**MODEM** jack on a splitter or your telephone wall jack.

Computers can connect to the ZyXEL Device's ETHERNET ports (or wirelessly).

Figure 1 ZyXEL Device's Internet Access Application



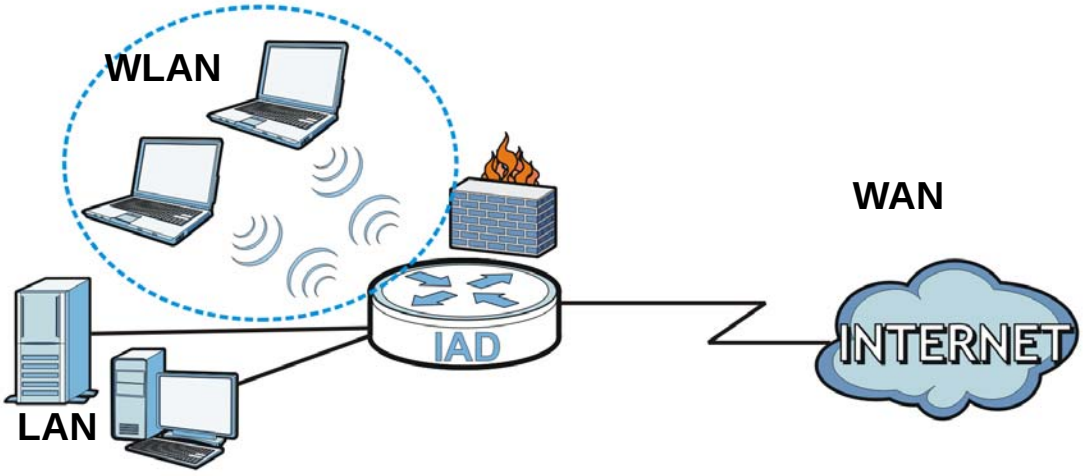
You can also configure the firewall on the ZyXEL Device for secure Internet access. When the firewall is on, all incoming traffic from the Internet to your network is blocked unless it is initiated from your network. This means that probes from the outside to your network are not allowed, but you can safely browse the Internet and download files.

Use QoS to efficiently manage traffic on your network by giving priority to certain types of traffic and/or to particular computers. For example, you could make sure that the ZyXEL Device gives email high priority, and/or limit bandwidth devoted to the boss's excessive file downloading.

1.2.2 Wireless Connection

By default, the wireless LAN (WLAN) is enabled on the ZyXEL Device. IEEE 802.11b/g/n compliant clients can wirelessly connect to the ZyXEL Device to access network resources. You can set up a wireless network with WPS (WiFi Protected Setup) or manually add a client to your wireless network.

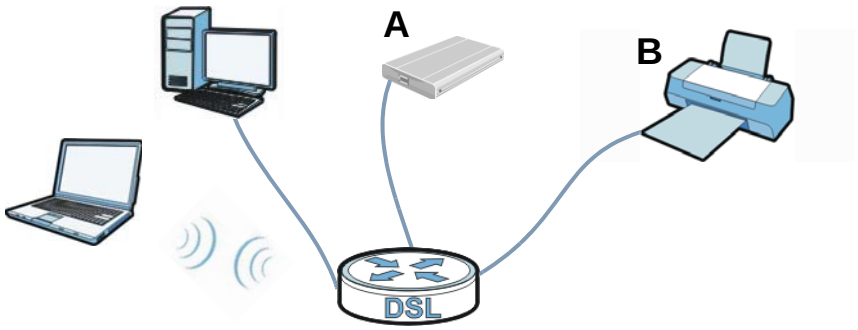
Figure 2 Wireless Connection Application



1.2.3 ZyXEL Device's USB and Print Server Support

Use the built-in USB 2.0 port to share files via a USB memory stick or a USB hard drive (**A**). Alternatively, you can add a USB printer (**B**) and make it available on your local area network.

Figure 3 USB File Sharing / Print Server Application



1.3 The WPS/WLAN Button

You can use the **WPS** button ( ) on the top of the device to turn the wireless LAN off or on. You can also use it to activate WPS in order to quickly set up a wireless network with strong security.

Turn the Wireless LAN On or Off

1 Make sure the **POWER** LED is on (not blinking).

2 Press the **WPS** button for one second and release it. The **WLAN / WPS** LED should change from off to on or vice versa.

Activate WPS

1 Make sure the **POWER** LED is on (not blinking).

2 Place the devices you want to connect near one another.

3 Press the **WPS** button on top of the ZyXEL Device for more than five seconds and release it to turn the WPS function on. Repeat this procedure when you want to turn the WPS function off.

4 Press the WPS button on another WPS -enabled device within range of the ZyXEL Device. The **WLAN / WPS** LED should flash while the ZyXEL Device sets up a WPS connection with the wireless device.

5 The **WLAN / WPS** light on the P-66xHNU-Fx Series shines steadily when connected.

Note: You must activate WPS in the ZyXEL Device and in another wireless device within two minutes of each other. See Chapter 6 on page 123 for more information.

1.4 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- FTP for firmware upgrades and configuration backup/restore.

1.5 Good Habits for Managing the ZyXEL Device

Do the following things regularly to make the ZyXEL Device more secure and to manage the ZyXEL Device more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the ZyXEL Device to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the ZyXEL Device. You could simply restore your last configuration.

Refer to the Quick Start Guide for information on hardware connections.

1.6 The RESET Button

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the device to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the passwords will be reset to the defaults.

1. Make sure the **POWER** LED is on (not blinking).
2. To set the device back to the factory default settings, press the **RESET** button for 5 seconds or until the **POWER** LED begins to blink and then release it. When the **POWER** LED begins to blink, the defaults have been restored and the device restarts.

2

Introducing the Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later versions, Mozilla Firefox 3 and later versions, or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

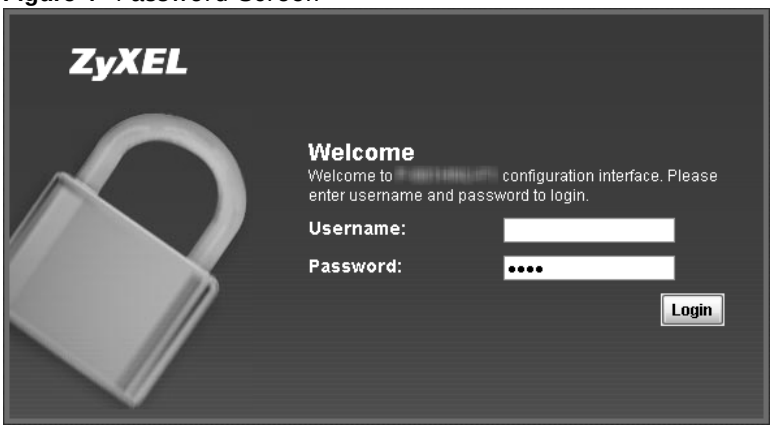
- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

See Appendix C on page 303 if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

1. Make sure your ZyXEL Device hardware is properly connected (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.1" as the URL.
4. A password screen displays. Type “admin” (default) as the username and “1234” as the password, and click **Login**. If you have changed the password, enter your password and click **Login**.

Figure 4 Password Screen



Note: For security reasons, the ZyXEL Device automatically logs you out if you do not use the web configurator for five minutes (default). If this happens, log in again.

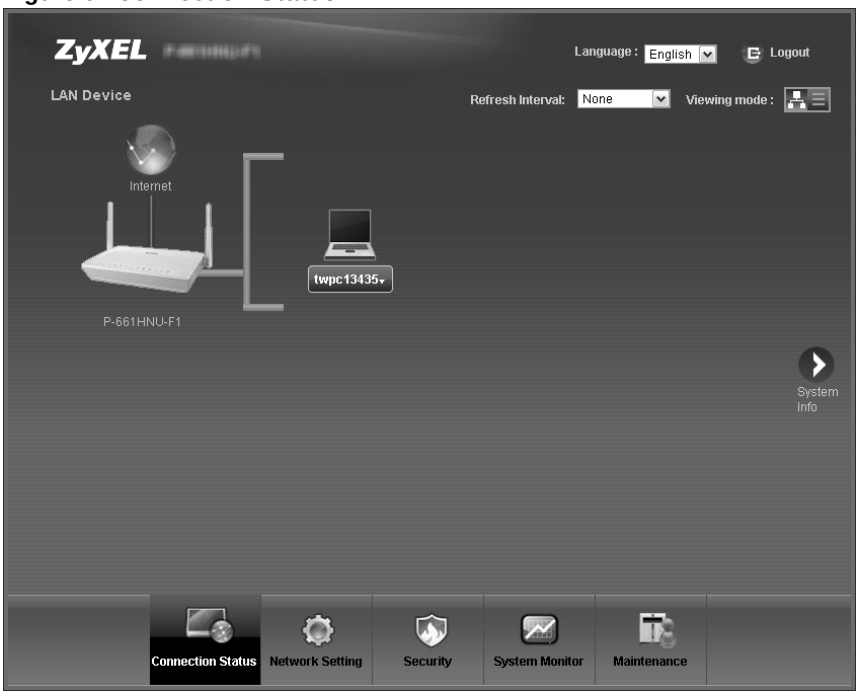
5 The following screen displays if you have not yet changed your password. It is strongly recommended you change the default password. Enter a new password, retype it to confirm and click **Apply**; alternatively click **Skip** to proceed to the Connection Status screen if you do not want to change the password now.

Figure 5 Change Password Screen


ZyXEL
Change Password
It is highly recommended to setup a new password instead of using the default one for security concern.
New Password:
Verify New Password:
Skip
Apply

6 The **Connection Status** screen appears. For P-660HNU-Fx and P-660HN-Fx, the Web Configurator is set to **User Mode** by default. See Section 2.3 on page 32 for more information on **User Mode**.

Figure 6 Connection Status



7 Click **System Info** to display the **System Info** screen, where you can view the ZyXEL Device's interface and system information.

2.2 The Web Configurator Layout

Click **Connection Status > System Info** to show the following screen.

Figure 7 Web Configurator Layout Screen



As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - main window
- **C** - navigation panel

2.2.1 Title Bar

The title bar shows the following icon in the upper right corner.



Click this icon to log out of the web configurator.

2.2.2 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

After you click **System Info** on the **Connection Status** screen, the **System Info** screen is displayed. See Chapter 4 on page 84 for more information about the **System Info** screen.

If you click **LAN Device** on the **System Info** screen, the **Connection Status** screen appears. See Chapter 4 on page 83 for more information about the **Connection Status** screen.

If you click **Virtual Device** on the **System Info** screen, a visual graphic appears, showing the connection status of the ZyXEL Device's ports. The connected ports are in color and disconnected ports are gray.

2.2.3 Navigation Panel

Use the menu items on the navigation panel to open screens to configure ZyXEL Device features. The following table describes each menu item.

Table 1 Navigation Panel Summary

LINK	TAB	FUNCTION
Connection Status		This screen shows the network status of the ZyXEL Device and computers/devices connected to it.
Network Setting		
Broadband	Broadband	Use this screen to view, remove or add a WAN interface. You can also configure ISP parameters, WAN IP address assignment, DNS servers and other advanced properties.
Wireless	General	Use this screen to turn the wireless connection on or off, specify the SSID(s) and configure the wireless LAN settings and WLAN authentication/security settings.
	More AP	Use this screen to configure multiple BSSs on the ZyXEL Device.
	WPS	Use this screen to use WPS (Wi-Fi Protected Setup) to establish a wireless connection.
	WMM	Use this screen to enable or disable Wi-Fi MultiMedia (WMM).
	Scheduling	Use this screen to configure when the ZyXEL Device enables or disables the wireless LAN.
Home Networking	LAN Setup	Use this screen to configure LAN TCP/IP settings, and other advanced properties.
	Static DHCP	Use this screen to assign specific IP addresses to individual MAC addresses.
	UPnP	Use this screen to enable the UPnP function.
	File Sharing	Use this screen to enable file sharing via the ZyXEL Device.
	Printer Server	Use this screen to enable or disable sharing of a USB printer via your ZyXEL Device.
Static Route	Static Route	Use this screen to view and set up static routes on the ZyXEL Device.
DNS Route	DNS Route	Use this screen to view and configure DNS routes.

Table 1 Navigation Panel Summary

LINK	TAB	FUNCTION
QoS	General	Use this screen to enable QoS and decide allowable bandwidth using QoS.
	Queue Setup	Use this screen to configure QoS queue assignment.
	Class Setup	Use this screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow.
	Monitor	Use this screen to view each queue's statistics.
NAT	Port Forwarding	Use this screen to make your local servers visible to the outside world.
	Sessions	Use this screen to limit the number of NAT sessions a single client can establish.
Dynamic DNS	Dynamic DNS	Use this screen to allow a static hostname alias for a dynamic IP address.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Services	Use this screen to set the default action to take on network traffic going in specific directions.
MAC Filter	MAC Filter	Use this screen to allow specific devices to access the ZyXEL Device.
Certificates	Local Certificates	Use this screen to generate and export self-signed certificates or certification requests and import the ZyXEL Device's CA-signed certificates.
	Trusted CAs	Use this screen to save CA certificates to the ZyXEL Device.
	VPN Certificates	Use this screen to import certificates and privates keys for VPN. Up to 4 certificates can be stored.
VPN	Setup	Use this screen to manage VPN settings
	Monitor	This page will show you the active tunnel's status
System Monitor		
Traffic Status	WAN	Use this screen to view the status of all network traffic going through the WAN port of the ZyXEL Device.
	LAN	Use this screen to view the status of all network traffic going through the LAN ports of the ZyXEL Device.
	NAT	Use this screen to view the status of NAT sessions on the ZyXEL Device.
Maintenance		
Users Account	Users Account	Use this screen to configure the passwords your user accounts.
Remote MGMT	Remote MGMT	Use this screen to enable specific traffic directions for network services.
System	System	Use this screen to configure the ZyXEL Device's name, domain name, management inactivity time-out.
Time Setting	Time Setting	Use this screen to change your ZyXEL Device's time and date.
Log Setting	Log Setting	Use this screen to select which logs and/or immediate alerts your device is to record. You can also set it to e-mail the logs to you.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your device.
Backup/Restore	Backup/Restore	Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.

Table 1 Navigation Panel Summary

LINK	TAB	FUNCTION
Reboot	Reboot	Use this screen to reboot the ZyXEL Device without turning the power off.
Diagnostic	Ping	Use this screen to test the connections to other devices.
	DSL Line	Use this screen to identify problems with the DSL connection.

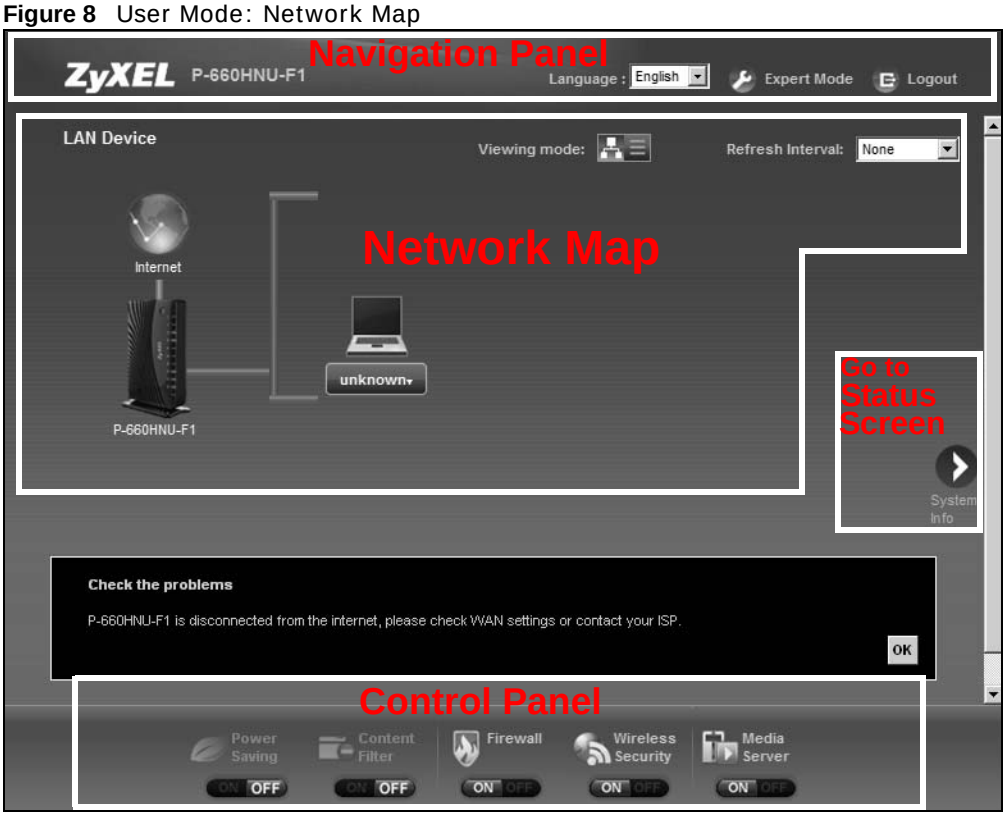
2.3 User Mode

2.3.1 Overview

The Web Configurator for P-660HNU-Fx and P-660HN-Fx is set to **User Mode** by default. You can configure several key features of the ZyXEL Device in this mode. This mode is useful to users who are not fully familiar with some features that are usually intended for network administrators.

When you log in to the Web Configurator, the following screen opens.

Figure 8 User Mode: Network Map



2.3.2 What You Can Do

You can do the following in this mode:

- Use this **Navigation Panel** to opt out of the **User** mode (Section 2.3.3 on page 33).

- Use the **Network Map** screen to check if your ZyXEL Device can ping the gateway and whether it is connected to the Internet (Section 2.3.4 on page 33).
- Use the **Control Panel** to configure and enable ZyXEL Device features, including wireless security, wireless scheduling and bandwidth management and so on (Section 2.3.5 on page 34).

2.3.3 Navigation Panel

Use this navigation panel to opt out of the **User** mode.

Figure 9 Control Panel



The following table describes the labels in this screen.

Table 2 Control Panel

ITEM	DESCRIPTION
Home	Click this to go to the **Login** page.
Expert Mode	Click this to change to **Expert** mode and customize features of the ZyXEL Device.
Logout	Click this to end the Web Configurator session.

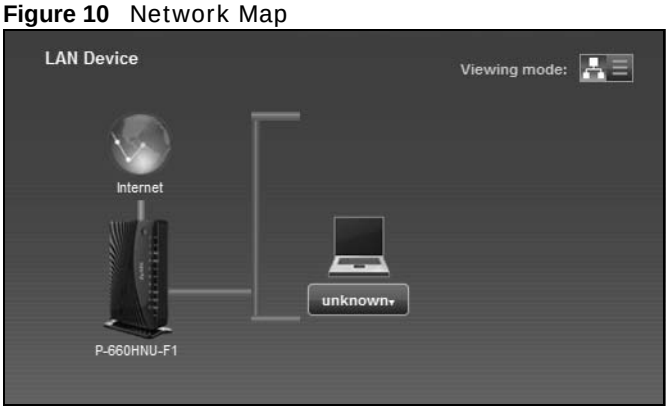
2.3.4 Network Map

Note: The Network MAP is viewable by Windows XP (need to install patch), Windows Vista and Windows 7 users only. For Windows XP (Service Pack 2) users, you can see the network devices connected to the ZyXEL Device by downloading the LLTD (Link Layer Topology Discovery) patch from the Microsoft Website.

Note: Don't worry if the Network Map does not display in your web browser. This feature may not be supported by your system. You can still configure the Control Panel (Section 2.3.5 on page 34) in the User Mode and the ZyXEL Device features that you want to use in the Expert Mode.

When you log into the Network Configurator, the Network Map is shown as follows.

Figure 10 Network Map



The line connecting the ZyXEL Device to the gateway becomes green when the ZyXEL Device is able to ping the gateway. It becomes red when the ping initiating from the ZyXEL Device does not get a

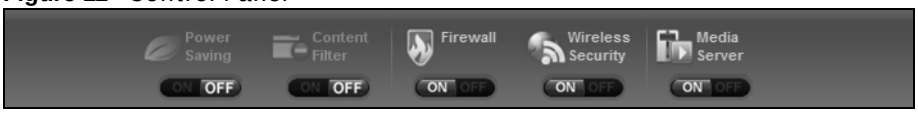
response from the gateway. The same rule applies to the line connecting the gateway to the Internet.

You can also view the devices (represented by icons indicating the kind of network device) connected to the ZyXEL Device, including those connecting wirelessly. Right-click on the ZyXEL Device icon to refresh the network map and go to the Wizard. Right click on the other icons to view information about the device.

2.3.5 Control Panel

The features configurable in **User Mode** are shown in the **Control Panel**.

Figure 11 Control Panel



Switch **ON** to enable the feature. Otherwise, switch **OFF**. If the feature is turned on, the green light flashes. If it is turned off, the red light flashes.

Additionally, click the feature to open a screen where you can edit its settings.

The following table describes the labels in this screen.

Table 3 Control Panel

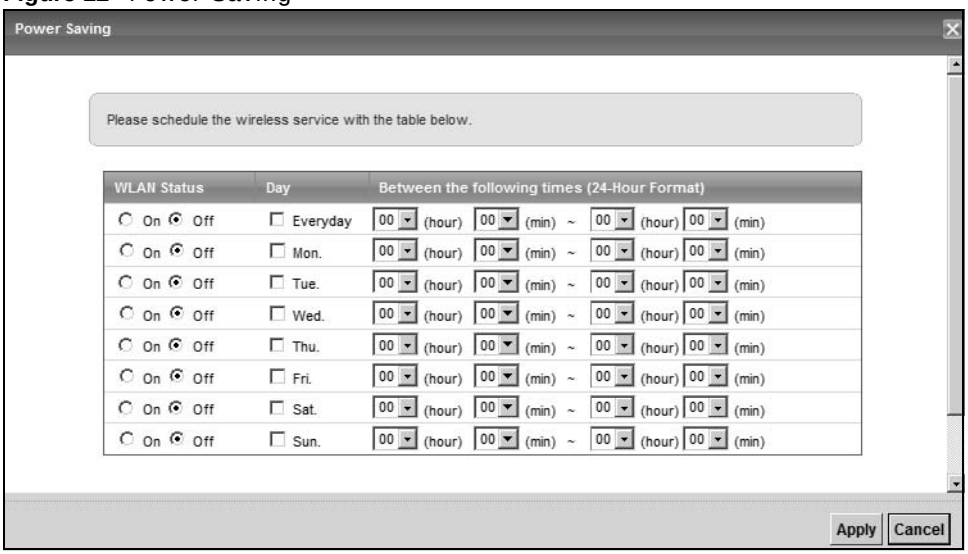
ITEM	DESCRIPTION
Power Saving	Click this to schedule the wireless feature of the ZyXEL Device. Disabling the wireless function helps lower the energy consumption of the ZyXEL Device. Switch **ON** to apply wireless scheduling. Otherwise, switch **OFF**. Refer to Section 2.3.6 on page 34 to see this screen.
Content Filter	Click this to restrict access to certain websites, based on keywords contained in URLs, to which you do not want users in your network to open. Switch **ON** to apply website filtering. Otherwise, switch **OFF**. Refer to Section 2.3.7 on page 35 to see this screen.
Firewall	Switch **ON** to ensure that your network is protected from Denial of Service (DoS) attacks. Otherwise, switch **OFF**. Refer to Section 2.3.8 on page 36 to see this screen.
Wireless Security	Click this to configure the wireless security, such as SSID, security mode and WPS key on your ZyXEL Device. Refer to Section 2.3.9 on page 37 to see this screen.
Media Server	Switch **ON** to enable the media server on your ZyXEL Device. Otherwise, switch **OFF**. Refer to Section 2.3.11 on page 38 to see this screen.

2.3.6 Power Saving

Use this screen to set the day of the week and time of the day when your wireless LAN is turned on and off. Wireless LAN scheduling is disabled by default.

Disabling the wireless capability lowers the energy consumption of the of the ZyXEL Device.

Figure 12 Power Saving



The following table describes the labels in this screen.

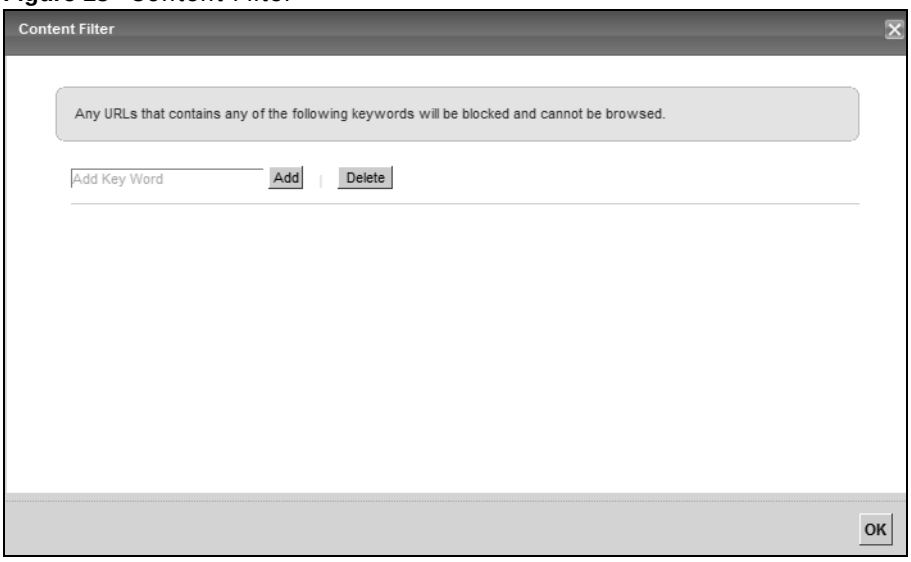
Table 4 Power Saving

LABEL	DESCRIPTION
WLAN Status	Select **On** or **Off** to specify whether the Wireless LAN is turned on or off (depending on what you selected in the **WLAN Status** field). This field works in conjunction with the **Day** and **For the following times** fields.
Day	Select **Everyday** or the specific days to turn the Wireless LAN on or off. If you select **Everyday** you can not select any specific days. This field works in conjunction with the **For the following times** field.
For the following times (24-Hour Format)	Select a begin time using the first set of **hour** and minute (**min**) drop down boxes and select an end time using the second set of **hour** and minute (**min**) drop down boxes. If you have chosen **On** earlier for the WLAN Status the Wireless LAN will turn on between the two times you enter in these fields. If you have chosen **Off** earlier for the WLAN Status the Wireless LAN will turn off between the two times you enter in these fields. In this time format, midnight is 00:00 and progresses up to 24:00. For example, 6:00 PM is 18:00.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to close this screen.

2.3.7 Content Filter

Use this screen to restrict access to certain websites, based on keywords contained in URLs, to which you do not want users in your network to open.

Figure 13 Content Filter


Content Filter
Any URLs that contains any of the following keywords will be blocked and cannot be browsed.
Add Key Word
Add
Delete
OK

The following table describes the labels in this screen.

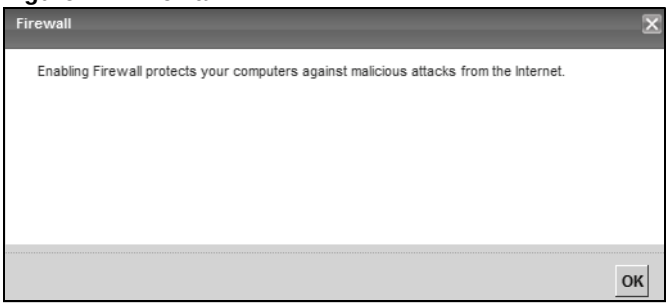
Table 5 Content Filter

LABEL	DESCRIPTION
Add	Click **Add** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. Note: The ZyXEL Device does not recognize wildcard characters as keywords. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the text box and click **Delete** to remove it. The keyword disappears from the text box after you click **Apply**.
OK	Click **OK** to save your changes.

2.3.8 Firewall

Enable this feature to protect the network from Denial of Service (DoS) attacks. The ZyXEL Device blocks repetitive pings from the WAN that can otherwise cause systems to slow down or hang.

Figure 14 Firewall

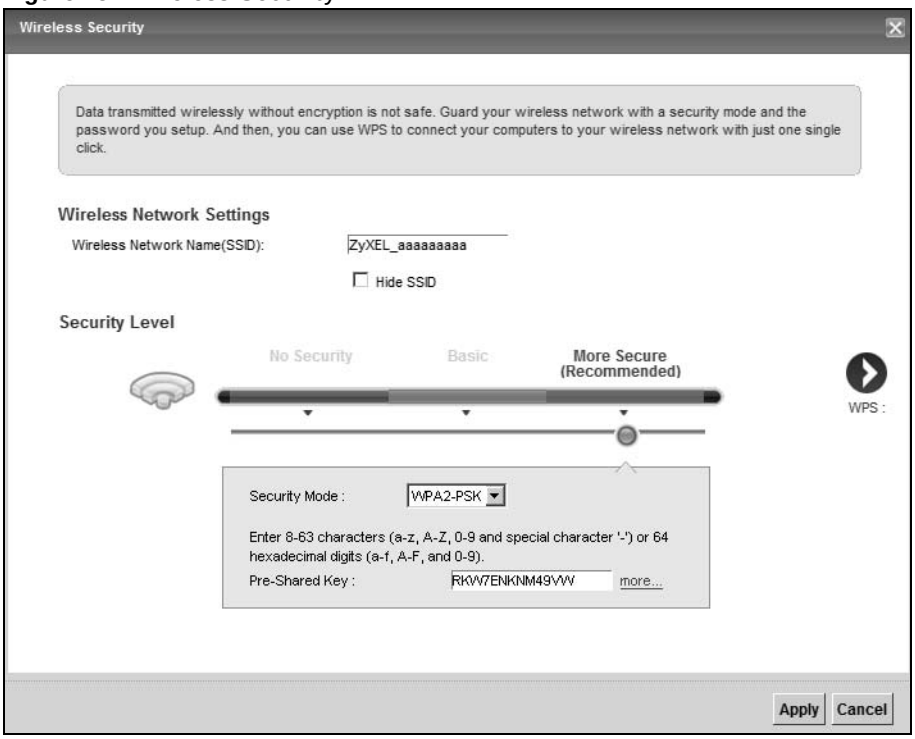


Click **OK** to close this screen.

2.3.9 Wireless Security

Use this screen to configure security for your the Wireless LAN. You can enter the SSID and select the wireless security mode in the following screen.

Figure 15 Wireless Security


Wireless Security
Data transmitted wirelessly without encryption is not safe. Guard your wireless network with a security mode and the password you setup. And then, you can use WPS to connect your computers to your wireless network with just one single click.
Wireless Network Settings
Wireless Network Name(SSID):
ZyXEL_aaaaaaaaa
Hide SSID
Security Level
No Security
Basic
More Secure (Recommended)
WPS :
Security Mode :
WPA2-PSK
Enter 8-63 characters (a-z, A-Z, 0-9 and special character '-') or 64 hexadecimal digits (a-f, A-F, and 0-9).
Pre-Shared Key :
RKW7ENKNM49VW
more...
Apply
Cancel

The following table describes the general wireless LAN labels in this screen.

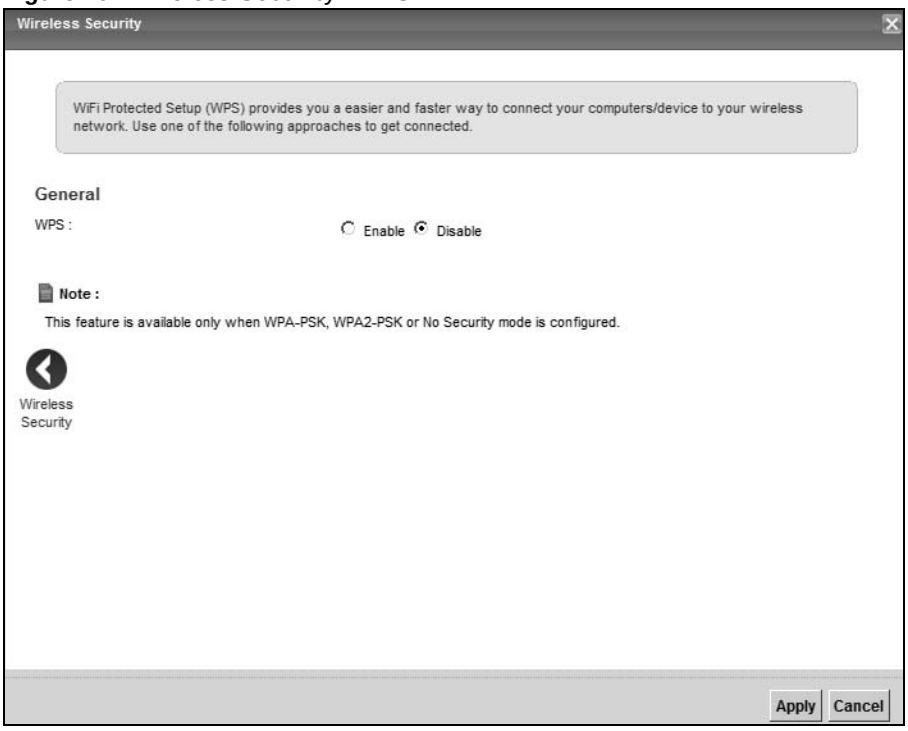
Table 6 Wireless Security

LABEL	DESCRIPTION
Wireless Network Name (SSID)	(Service Set IDentity) The SSID identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 keyboard characters) for the wireless LAN.
Security Mode	Select **Basic** or **More Secure** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the ZyXEL Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See Section 6.2 on page 107 for more details about wireless security modes.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to close this screen.
WPS	Click this to configure the WPS screen. You can transfer the wireless settings configured here (**Wireless Security** screen) to another wireless device that supports WPS.

2.3.10 WPS

Use this screen to add a wireless station to the network using WPS. Click **WPS** in the **Wireless Security** to open the following screen.

Figure 16 Wireless Security: WPS


Wireless Security
WiFi Protected Setup (WPS) provides you a easier and faster way to connect your computers/device to your wireless network. Use one of the following approaches to get connected.
General
WPS :
Enable
Disable
Note :
This feature is available only when WPA-PSK, WPA2-PSK or No Security mode is configured.
Wireless Security
Apply
Cancel

The following table describes the labels in this screen.

Table 7 Wireless Security: WPS

LABEL	DESCRIPTION
Wireless Security	Click this to go back to the **Wireless Security** screen.
Enable WPS	Select **Enable** to activate WPS on the ZyXEL Device.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to close this screen.

2.3.11 Media Server

You can set up your ZyXEL Device to act as a media server to provide media (like video) to DLNA-compliant players, such as Windows Media Player, ZyXEL DMAs (Digital Media Adapters), Xboxes or PS3s. The media server and the clients must have IP addresses in the same subnet. See Section 7.6 on page 142 for more information on the Media Server feature.

If you would like to play any media contents stored in a USB flash drive or disk through a media client, like PS3, attach the USB flash drive or disk onto this device and enable the Media Server function.

Figure 17 Media Server


Media Server
If you would like to play any media contents stored in a USB flash drive or disk through a media client, like PS3, attach the USB flash drive or disk onto this device and enable the Media Server function.
OK

Click **OK** to close this screen.

3

Tutorials

3.1 Overview

This chapter contains the following tutorials:

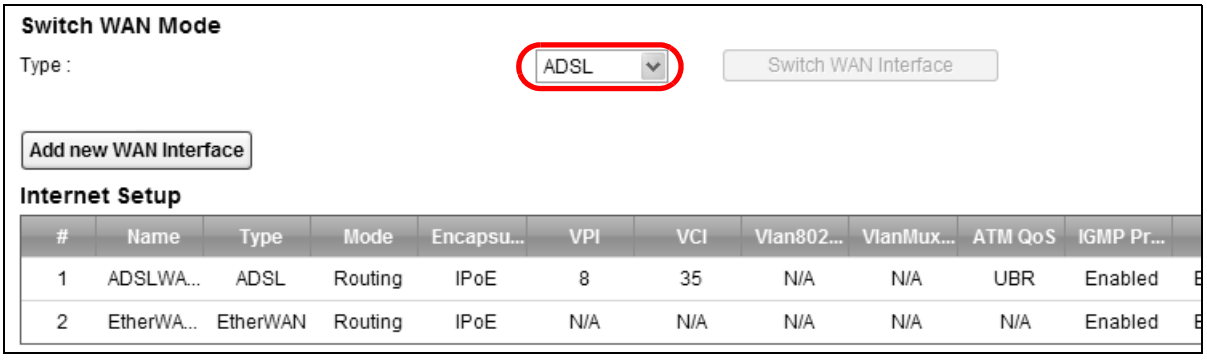
- Setting Up Your DSL Connection
- How to Set up a Wireless Network
- Setting Up NAT Port Forwarding to Allow Access to Network Servers from the Internet
- Using the File Sharing Feature
- Using the Print Server Feature
- Configuring the MAC Address Filter for Restricting Wireless Internet Access
- Configuring Static Route for Routing to Another Network
- Configuring QoS Queue and Class Setup
- Access the ADSL Device Using DDNS

3.2 Setting Up Your DSL Connection

This tutorial shows you how to set up your ADSL settings for Internet connection using the Web Configurator. If you connect to the Internet through a DSL connection, connect the ADSL Device properly. Refer to the Quick Start Guide for details on the ADSL Device's hardware connections.

PPPoE Account Configuration

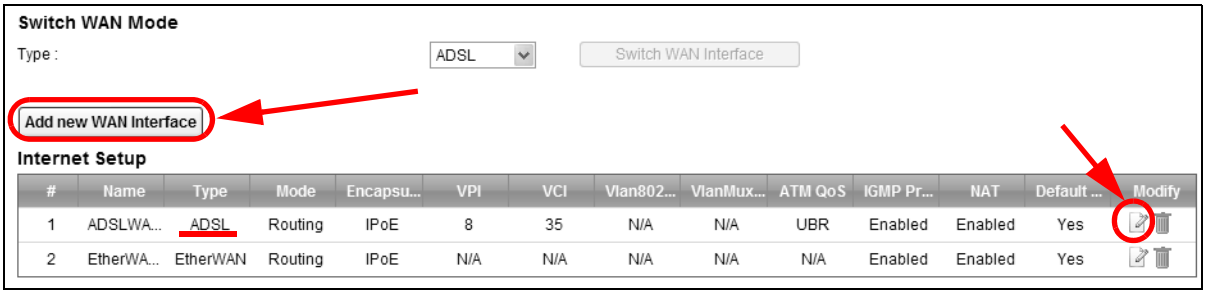
1 Click **Network Setting > Broadband** to open the screen shown below. Make sure you select **ADSL** in the **Type** field.


Switch WAN Mode
Type :
ADSL
Switch WAN Interface
Add new WAN Interface
Internet Setup
Name Type Mode Encapsu... VPI VCI Vlan802... VlanMux... ATM QoS IGMP Pr...
1 ADSLWA... ADSL Routing IPoE 8 35 N/A N/A UBR Enabled
2 EtherWA... EtherWAN Routing IPoE N/A N/A N/A N/A N/A Enabled

Note: If the type is **EtherWAN**, select **ADSL** and click the **Switch WAN Interface** button. The ADSL Device will switch to ADSL mode after it restarts.

2 You can either modify the default ADSL WAN interface by clicking the **Edit** icon or create a new WAN interface (if you want to keep the default one). This example creates a new WAN interface.

Click **Add new WAN Interface**.

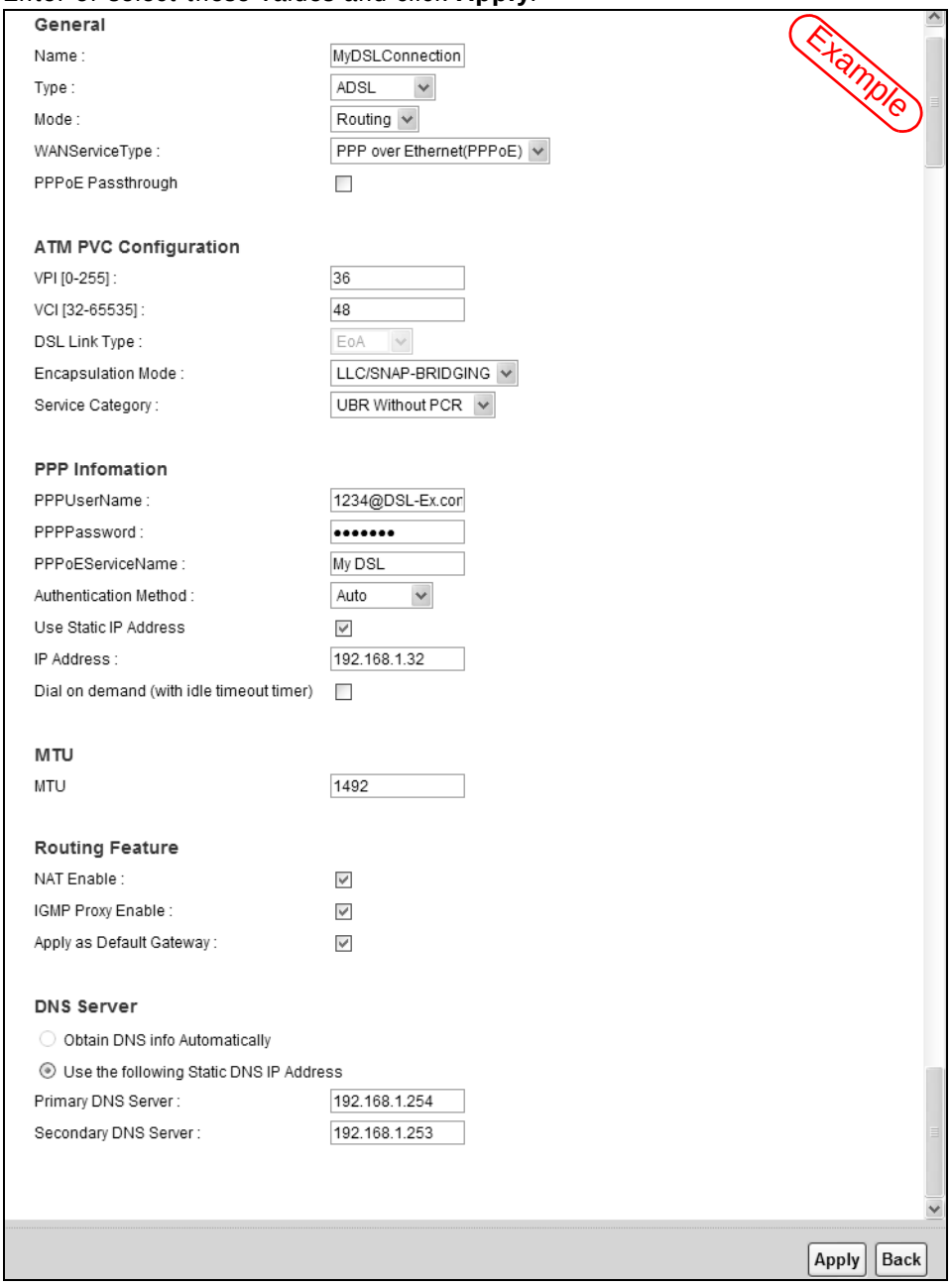

Switch WAN Mode
Type :
ADSL
Switch WAN Interface
Add new WAN Interface
Internet Setup
Name Type Mode Encapsu... VPI VCI Vlan802... VlanMux... ATM QoS IGMP Pr... NAT Default ... Modify
1 ADSLWA... ADSL Routing IPoE 8 35 N/A N/A UBR Enabled Enabled Yes
2 EtherWA... EtherWAN Routing IPoE N/A N/A N/A N/A N/A Enabled Enabled Yes

Note: You can create multiple ADSL WAN interfaces, however, only one of them is active at one time. The **Default Gateway** field in the table indicates the interface is active (**Yes**) or not (**No**).

3 For this example, the interface type is ADSL and the connection has the following information.

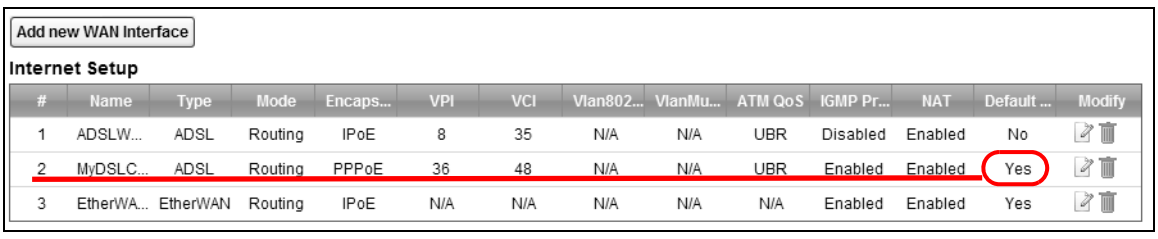
General	
Name	MyDSLConnection
Type	ADSL
Mode	Routing
WAN Service Type	PPP over Ethernet (PPPoE)
ATM PVC Configuration	
VPI/VCI	36/48
Encapsulation Mode	LLC/SNAP-BRIDGING
Service Category	UBR without PCR
PPP Information	
PPP User Name	1234@DSL-Ex.com
PPP Password	ABCDEF!
PPPoE Service Name	My DSL
Authentication Method	Auto
Static IP Address	Put a check on the option **Use Static IP Address**. Use 192.168.1.32 as the IP Address.
Others	PPPoE Passthrough: Disabled NAT: Enabled IGMP Proxy: Enabled Apply as Default Gateway: Enable DNS Server: Static DNS IP Address (Primary: 192.168.1.254 Secondary: 192.168.1.253)

Enter or select these values and click **Apply**.



This completes your DSL WAN connection setting.

4 You should see a summary of your new DSL connection setup in the **Broadband** screen as follows. The ADSL WAN interface you just created should be active (**Yes** in the **Default Gateway** field).



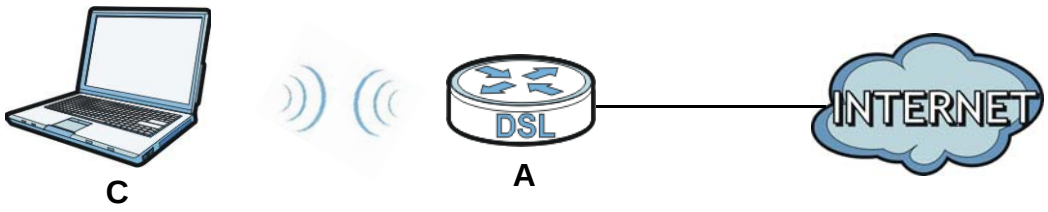
#	Name	Type	Mode	Encaps...	VPI	VCI	Vlan802...	VlanMu...	ATM QoS	IGMP Pr...	NAT	Default ...	Modify
1	ADSLW...	ADSL	Routing	IPoE	8	35	N/A	N/A	UBR	Disabled	Enabled	No	
2	MyDSLC...	ADSL	Routing	PPPoE	36	48	N/A	N/A	UBR	Enabled	Enabled	Yes	
3	EtherWA...	EtherWAN	Routing	IPoE	N/A	N/A	N/A	N/A	N/A	Enabled	Enabled	Yes	

Try to connect to a website, such as “www.zyxel.com” to see if you have correctly set up your Internet connection. Be sure to contact your service provider for any information you need to configure the WAN screens.

3.3 How to Set up a Wireless Network

This section gives you examples of how to connect the Internet wirelessly through the ADSL Device. A wireless network card or USB wireless adapter is referred to as the “wireless client” here.

In the following diagram, the wireless client is labeled **C** and the ADSL Device is labeled **A**.



Note: This section shows how to set up the wireless client using two methods: using the Microsoft Windows utility and the WPS PIN method. Refer to the Quick Start Guide if the wireless client has a WPS button and you wish to connect wirelessly using another WPS button method (Push Button Configuration).

3.3.1 Example Parameters

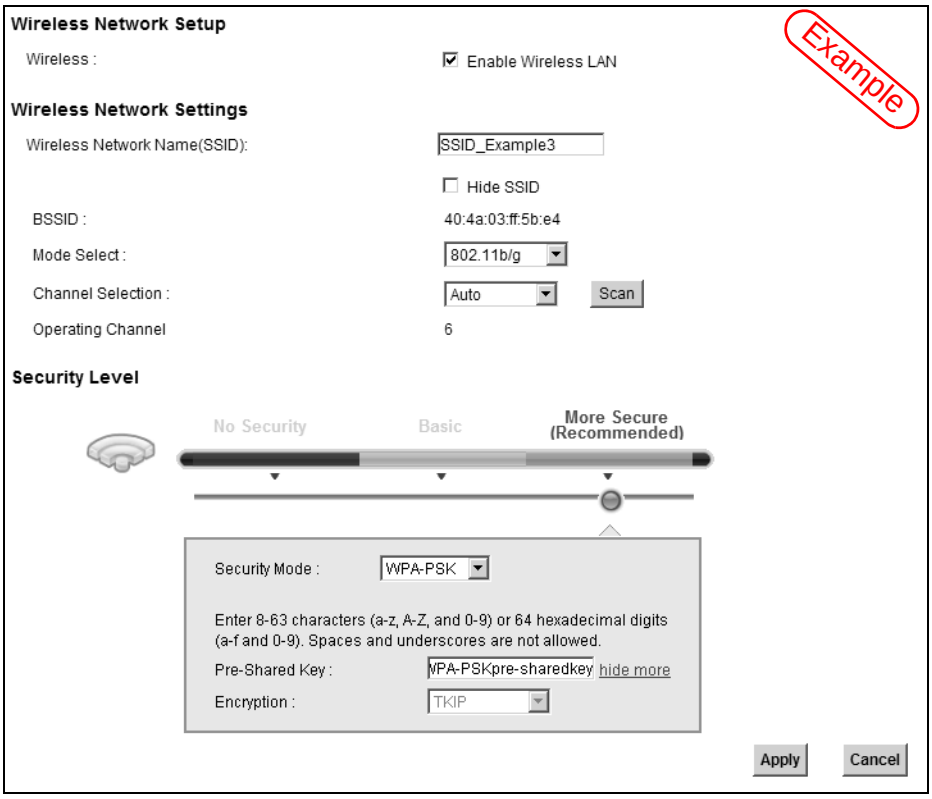
The following parameters will be used to configure the ADSL Device.

SSID	SSID_Example3
802.11 mode	802.11b/g
Channel	auto
Security	WPA-PSK (Pre-Shared Key: ThisismyWPA-PSKpre-sharedkey)

3.3.2 Configuring the ADSL Device

Follow the steps below to configure the wireless settings on your ADSL Device.

1 Open the **Network Setting > Wireless > General** screen in the ADSL Device’s web configurator.



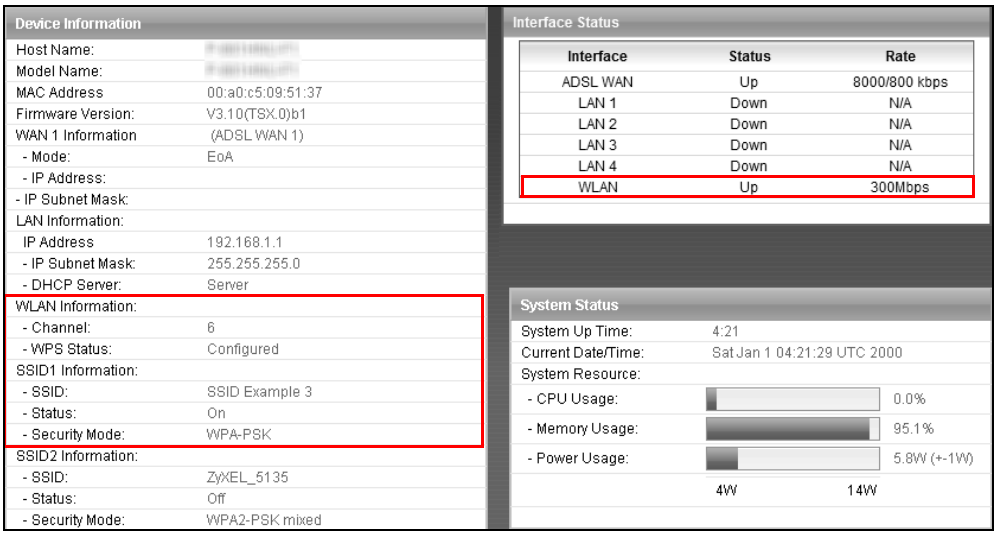
2 Make sure **Enable Wireless LAN** is selected.

3 Enter “SSID_Example3” as the SSID and select **Auto** in the **Channel Selection** field to have the device search for an available channel.

4 Select **802.11b/g** in the **Mode Select** field.

5 Select **More Secure** as your security level and set security mode to **WPA-PSK** and enter “ThisismyWPA-PSKpre-sharedkey” in the **Pre-Shared Key** field. Click **Apply**.

6 Click **Connection Status > System Info**. Verify your wireless and wireless security settings under **Device Information** and check if the WLAN connection is up under **Interface Status**.

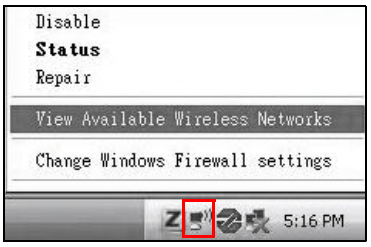


This finishes the configuration of the ADSL Device.

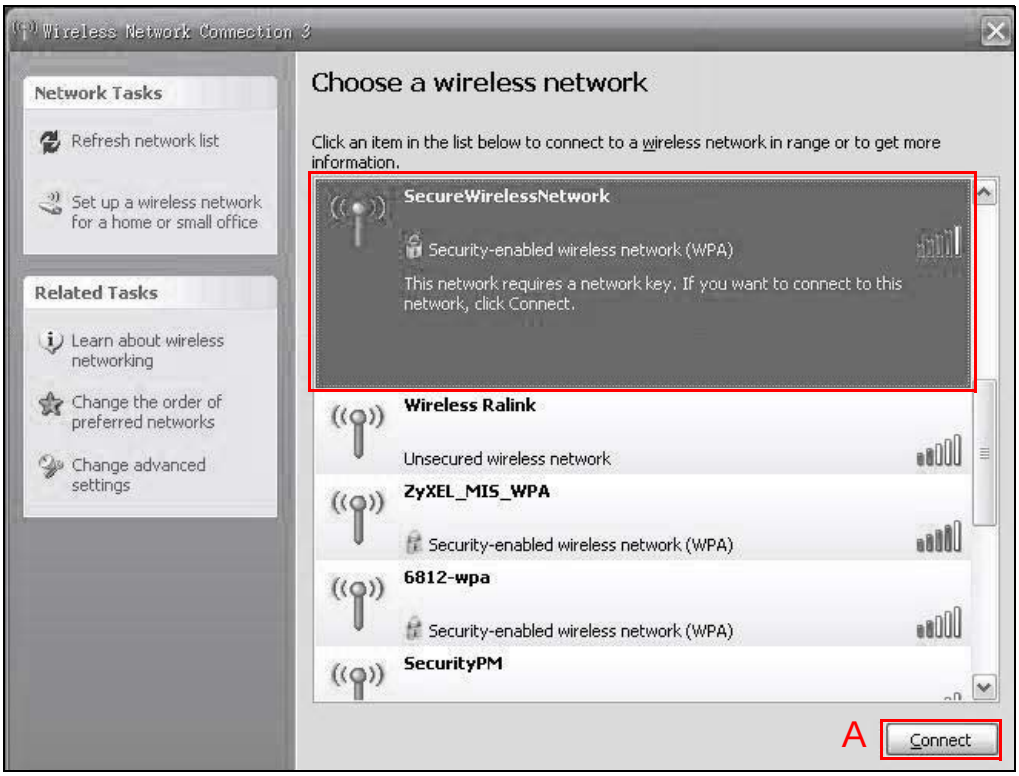
3.3.3 Connecting Wirelessly to your ADSL Device

This section describes how to connect wirelessly to your ADSL Device. The connection procedure is shown here using Windows XP as an example.

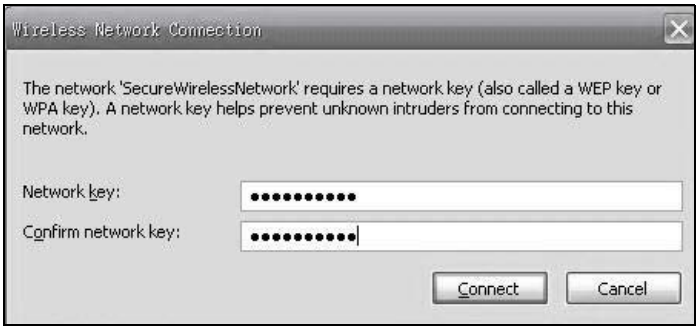
1 Right-click the wireless adapter icon which appears in the bottom right of your computer monitor. Click **View Available Wireless Networks**.



2 Select the ADSL Device's **SSID** name and click **Connect** (A). The SSID "SecureWirelessNetwork" is given here as an example.


Wireless Network Connection 3
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Choose a wireless network
Click an item in the list below to connect to a wireless network in range or to get more information.
SecureWirelessNetwork
Security-enabled wireless network (WPA)
This network requires a network key. If you want to connect to this network, click Connect.
Wireless Ralink
Unsecured wireless network
ZyXEL_MIS_WPA
Security-enabled wireless network (WPA)
6812-wpa
Security-enabled wireless network (WPA)
SecurityPM
A
Connect

3 You are prompted to enter a password. Enter it (the pre-shared key) and click **Connect**.


Wireless Network Connection
The network 'SecureWirelessNetwork' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.
Network key:
Confirm network key:
Connect
Cancel

4 You may have to wait several minutes while your computer connects to the wireless network.

5 You should now be securely connected wirelessly to the ADSL Device.



Congratulations! Your computer is now ready to connect to the Internet wirelessly through your ADSL Device.

Note: If you cannot connect wirelessly to the ADSL Device, check you have selected the correct SSID and entered the correct security key. If that does not work, ensure your wireless network adapter is enabled by clicking on the wireless adapter icon and clicking Enable.

3.3.4 Configuring the Wireless Client using the WPS PIN number

This section describes how to connect the wireless client to a network using the WPS PIN method. You need to log into the Web Configurator for this.

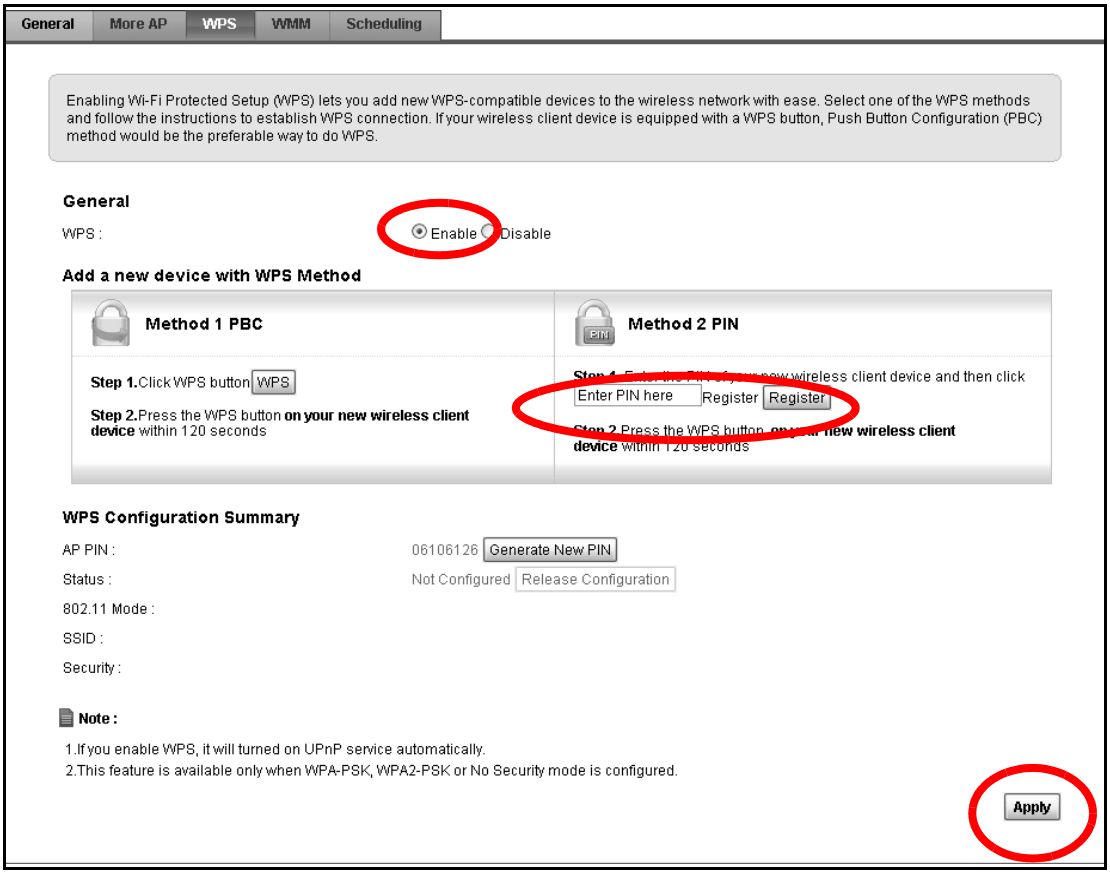
1 Place a WPS-enabled device that supports the WPS PIN configuration method near the ADSL Device.

2 Log into the ADSL Device's web configurator at **http://192.168.1.1** (see **Introducing the Web Configurator** on page 27 for more details on this).

3 In the navigation panel, click **Network Setting > Wireless > WPS**.

4 Select the **Enable** check box and click **Apply** to enable the WPS function.

5 Enter the PIN of the other WPS-enabled device into the **Enter PIN here** text box and click **Register**. You can locate this PIN number in the other device's utility or on the device itself. See the other device's documentation if you cannot locate the PIN.


General
More AP
WPS
WMM
Scheduling
Enabling Wi-Fi Protected Setup (WPS) lets you add new WPS-compatible devices to the wireless network with ease. Select one of the WPS methods and follow the instructions to establish WPS connection. If your wireless client device is equipped with a WPS button, Push Button Configuration (PBC) method would be the preferable way to do WPS.
General
WPS :
Enable
Disable
Add a new device with WPS Method
Method 1 PBC
Step 1.Click WPS button
WPS
Step 2.Press the WPS button on your new wireless client device within 120 seconds
Method 2 PIN
Enter PIN here
Register
Register
device within 120 seconds
WPS Configuration Summary
AP PIN :
06106126
Generate New PIN
Status :
Not Configured
Release Configuration
802.11 Mode :
SSID :
Security :
Note :
1.If you enable WPS, it will turned on UPnP service automatically.
2.This feature is available only when WPA-PSK, WPA2-PSK or No Security mode is configured.
Apply

6 Click **Start** or **Apply** in the other device's utility screen within two minutes of clicking **Register** in the ADSL Device web configurator screen.

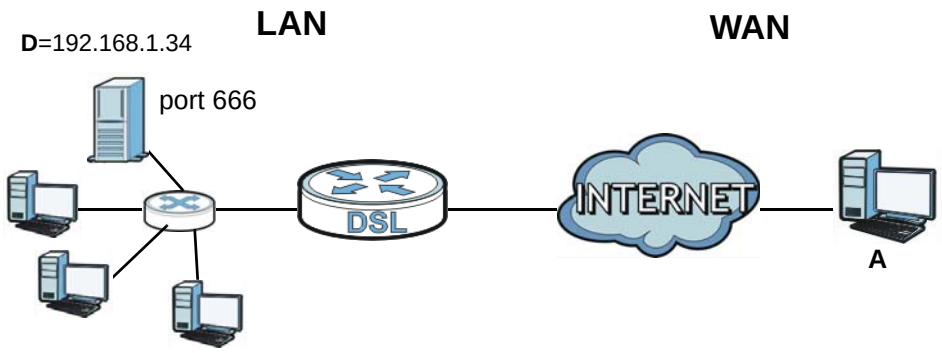
7 The ADSL Device and the other WPS-enabled device establish a secure connection. This can take up to two minutes.

8 Your computer is now ready to connect to the Internet wirelessly through your ADSL Device.

Note: You must repeat this procedure for every device you want to add to your network using WPS.

3.4 Setting Up NAT Port Forwarding to Allow Access to Network Servers from the Internet

In this tutorial, you manage the Doom server on a computer behind the ADSL Device. In order for players on the Internet (like **A** in the figure below) to communicate with the Doom server, you need to configure the port settings and IP address on the ADSL Device. Traffic should be forwarded to the port 666 of the Doom server computer which has an IP address of 192.168.1.34.

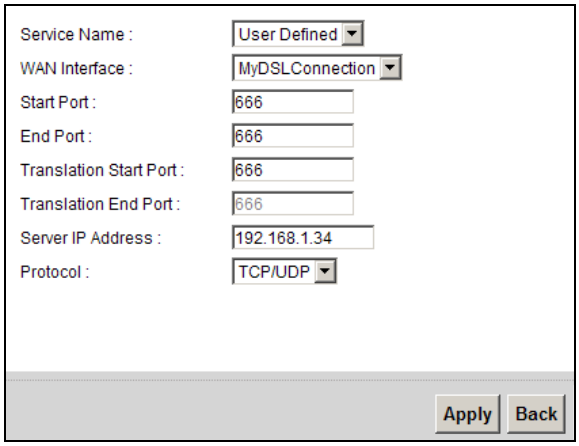


You may set up the port settings by configuring the port settings for the Doom server computer (see Chapter 11 on page 176 for more information).

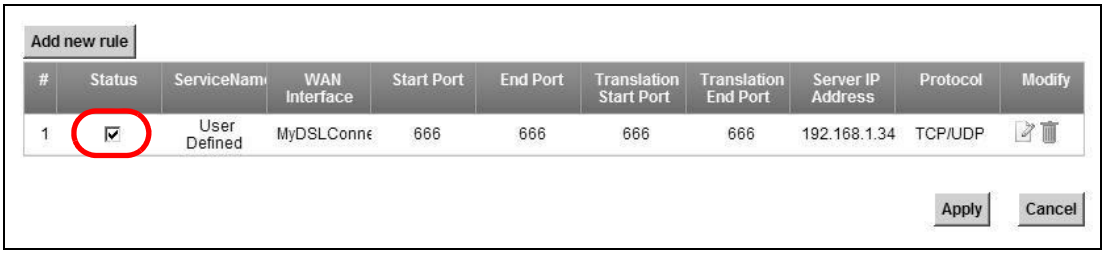
1 Click **Network Setting** > **NAT** > **Port Forwarding**. Click **Add new rule**.

2 Enter the following values and then click **Apply**.

Service Name	Select **User Defined**.
WAN Interface	Select the WAN interface through which the Doom service is forwarded. This is the default interface for this example, which is **MyDSLConnection**.
Start/End Ports	**666**
Translation Start/End Ports	**666**
Server IP Address	Enter the IP address of the Doom server. This is **192.168.1.34** for this example.
Protocol	Select **TCP/UDP**. This should be the protocol supported by the Doom server.



3 The port forwarding settings you configured should appear in the table. Make sure the **Status** check box for this rule is selected. Click **Apply** to have the ADSL Device start forwarding port 666 traffic to the computer with IP address 192.168.1.34.


Add new rule
Status ServiceNam WAN Interface Start Port End Port Translation Start Port Translation End Port Server IP Address Protocol Modify
1 User Defined MyDSLConne 666 666 666 666 192.168.1.34 TCP/UDP
Apply
Cancel

Players on the Internet then can have access to your Doom server.

3.5 Using the File Sharing Feature

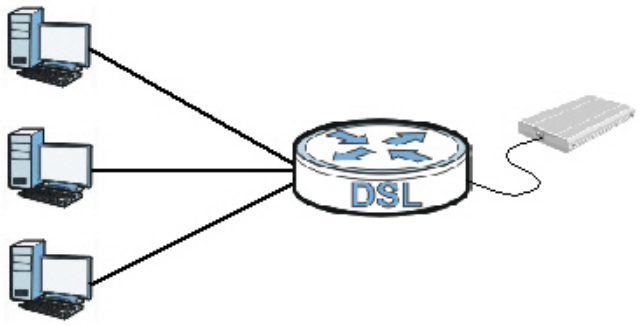
In this section you can:

- Set up file sharing to allow a USB storage device connected to the ADSL Device to be used by all users in your LAN as if it was directly connected to their computers.
- Access the shared files on the USB storage device from a LAN computer.

Suppose Bob has a USB drive containing **Bob_public** and **Bob_private** folders.

Bob_public contains general files everyone in the network can access.

Bob_private should only be accessible to Bob.



Note: Remember to control physical access to the USB drive so someone doesn't access files by simply connecting it to a computer.

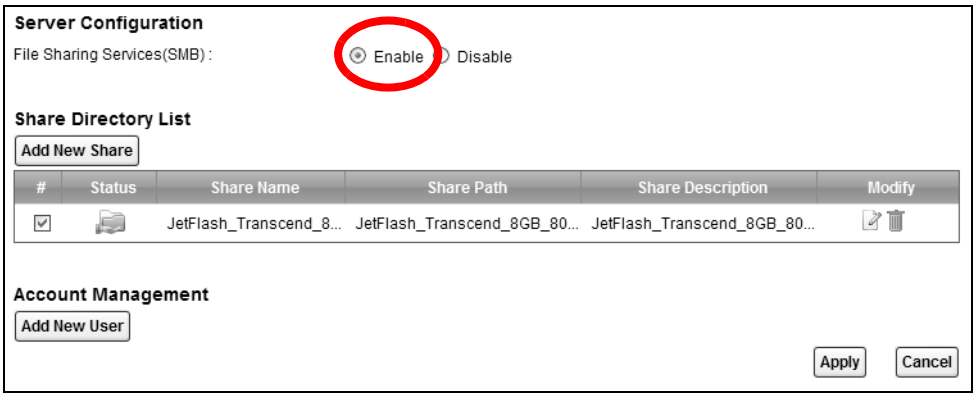
3.5.1 Set Up File Sharing

To set up file sharing you need to connect your USB device, create user account(s) (only if you want to restrict a share's access to certain users), enable file sharing and set up your share(s).

3.5.1.1 Activate File Sharing

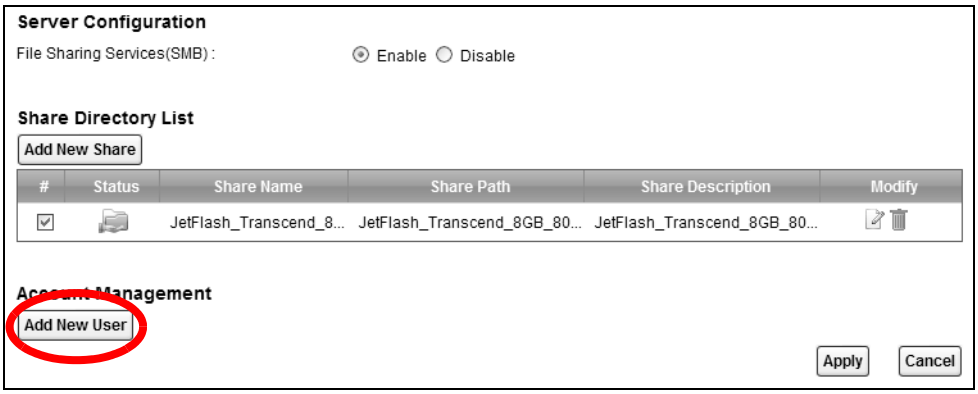
1 Connect your USB device to the USB port at the back panel of the ADSL Device.

2 In Expert mode, click **Network Setting > Home Networking > File Sharing**. Select **Enable** and click **Apply** to activate the file sharing function. The ADSL Device automatically adds your USB device to the **Share Directory List**.

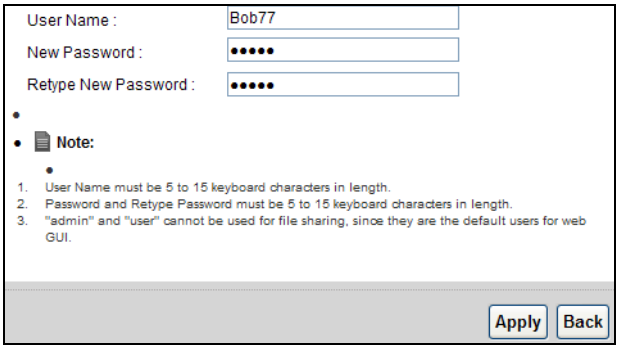


3.5.1.2 Create User Account(s)

1 If you wish to create users and grant them access to specific shares, click **Add New User** in the **File Sharing** screen.



2 Enter a user name. A user name can be any combination of letters and numbers. It must be between 5 and 15 characters long. This examples uses **Bob77** as the username.


User Name :
Bob77
New Password :
Retype New Password :
Note:
1. User Name must be 5 to 15 keyboard characters in length.
2. Password and Retype Password must be 5 to 15 keyboard characters in length.
3. "admin" and "user" cannot be used for file sharing, since they are the default users for web GUI.
Apply
Back

3 Enter the password that this user name must type when accessing the share. Retype it in the field below for confirmation. A password can be any combination of letters and numbers. It is case sensitive and it must be between 5 and 15 characters long.

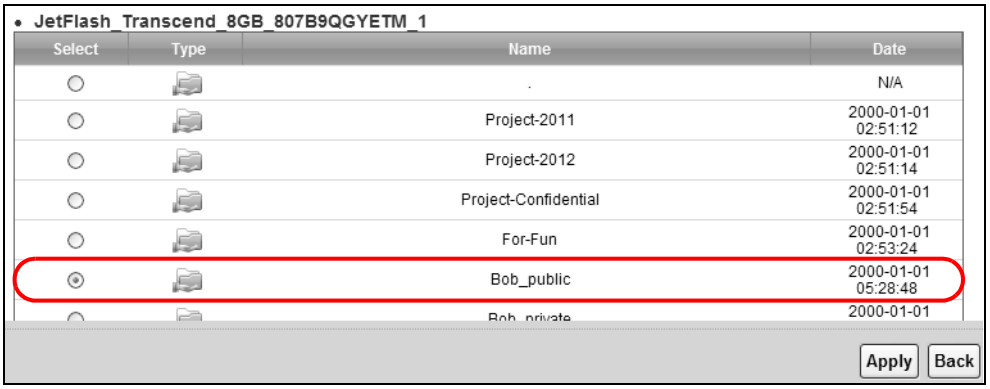
3.5.1.3 Set up File Sharing on Your ADSL Device

You also need to set up file sharing on your ADSL Device in order to share files.

1 Click **Add new share** in the **File Sharing** screen.

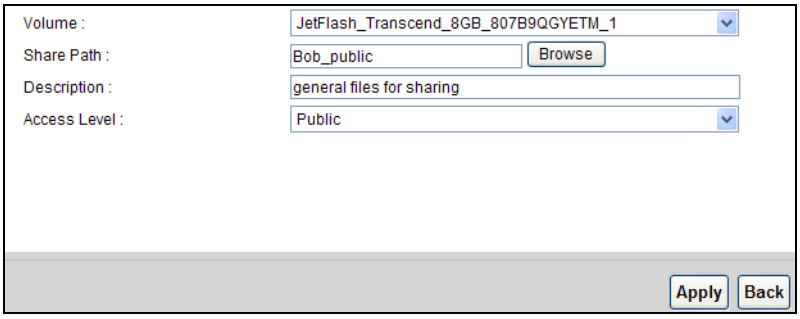
2 Click **Browse** to browse through all the files on your USB device.

3 Select the folder that you want to add as a share. In this example, select **Bob_public**. Click **Apply**.

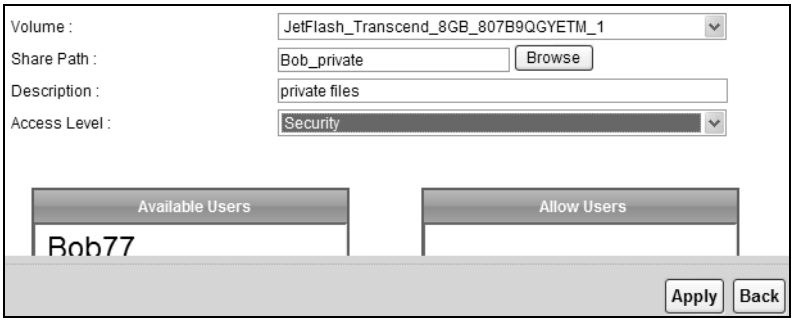


Note: Select the first option on this list to include all files and folders on the USB device.

4 You can add a description for the share or leave it blank. The **Add Share Directory** screen should look like the following. Leave the **Access Level** as **Public** to allow anyone connected to the ADSL Device to access the share. Click **Apply**.

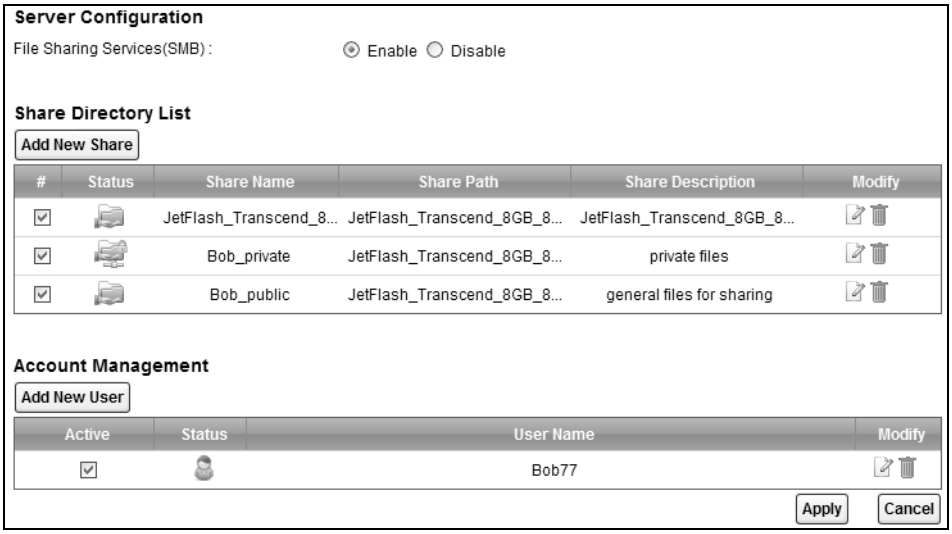


5 Click **Add new share** again in the **File Sharing** screen. This time, you select the **Bob_private** folder which contains important files. You want to restrict access to the share to certain users, (**Bob77** in this example). So select **Security** as the **Access Level**.

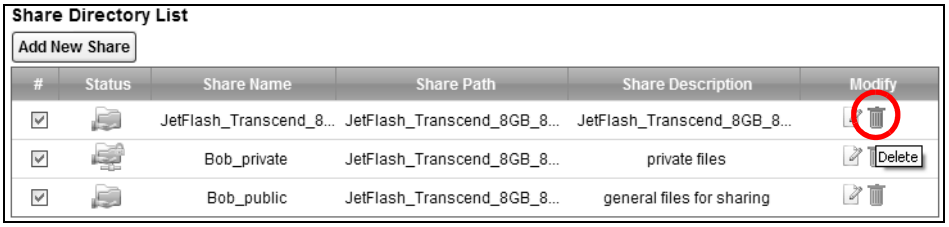


6 Select user **Bob77** from the **Available Users** list. Click on the arrows between the **Available Users** and **Allow Users** boxes to grant or deny access to the specific share that you are adding. Only users listed under **Allow Users** can access the share. Click **Apply** to finish.

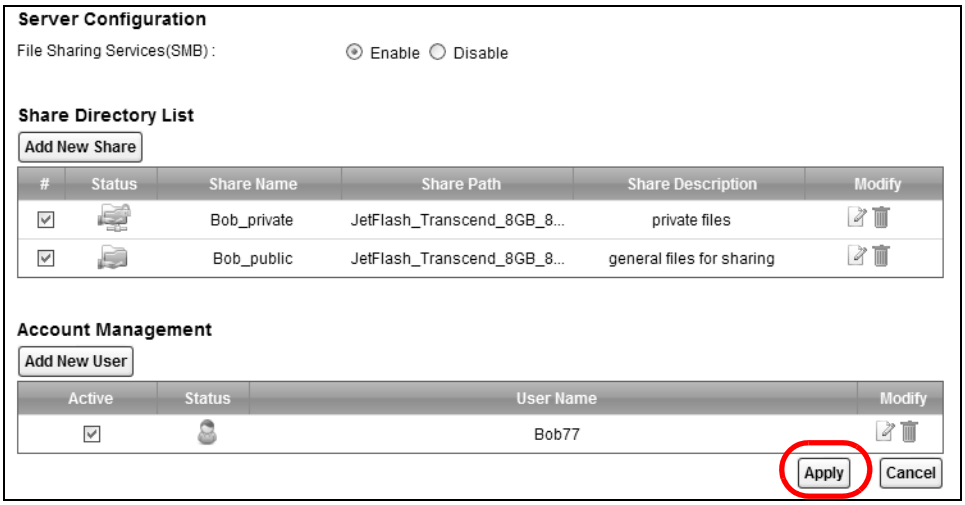
7 This sets up the file sharing server. You can see three shares listed in the table as shown.



8 Because you just want to share the **Bob_private** and **Bob_public** folders, you don't need the first share the system created, which shares the whole USB drive with everyone. So click the entry's **Delete** icon and confirm the delete action.


Share Directory List
Add New Share
Status Share Name Share Path Share Description Modify
JetFlash_Transcend_8... JetFlash_Transcend_8GB_8... JetFlash_Transcend_8GB_8...
Bob_private JetFlash_Transcend_8GB_8... private files
Bob_public JetFlash_Transcend_8GB_8... general files for sharing
Delete

9 Finally, click **Apply** again to save the changes.



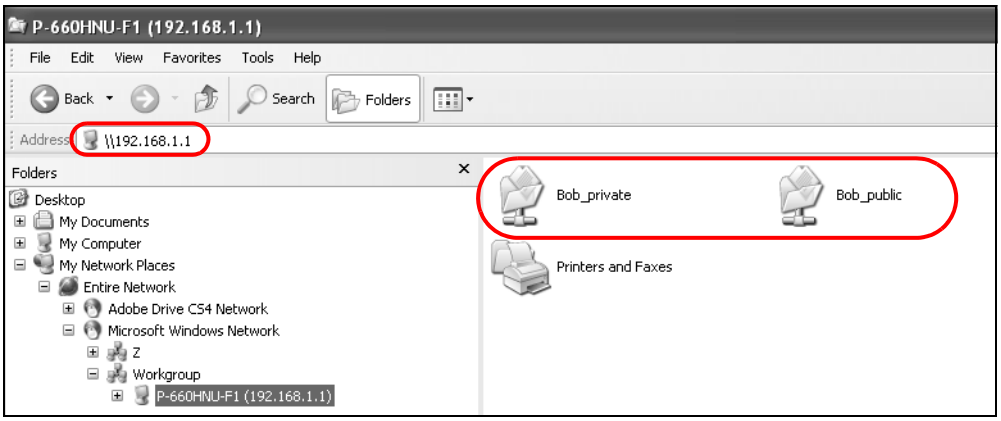
3.5.2 Access Your Shared Files From a Computer

You can use Windows Explorer to access the file storage devices connected to the ADSL Device.

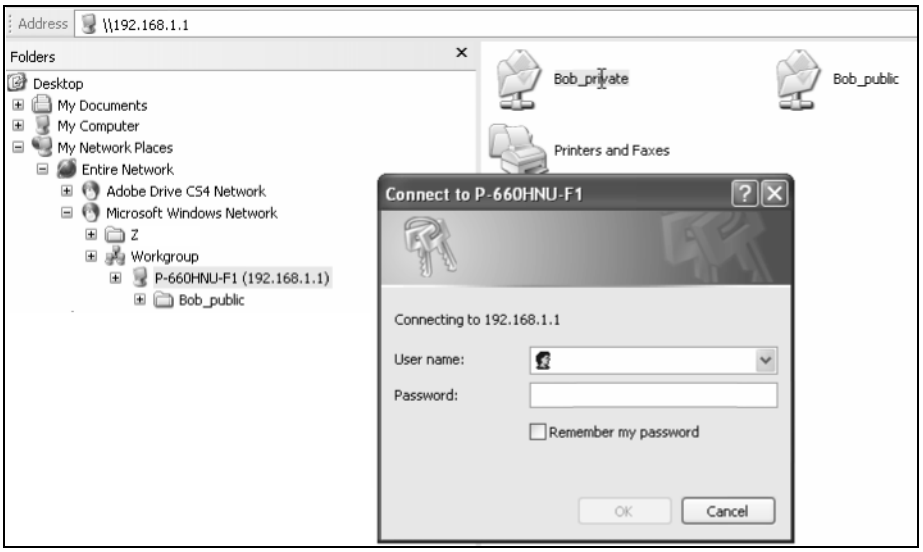
Note: The examples in this User's Guide show you how to use Microsoft's Windows XP to browse your shared files. Refer to your operating system's documentation for how to browse your file structure.

1 Open Windows Explorer on a computer which is connected to the ADSL Device's LAN port.

2 In Windows Explorer's Address bar type a double backslash "\\" followed by the IP address of the ADSL Device (the default IP address of the ADSL Device is 192.168.1.1) and press [ENTER]. The share folders **Bob_public** and **Bob_private** are available.



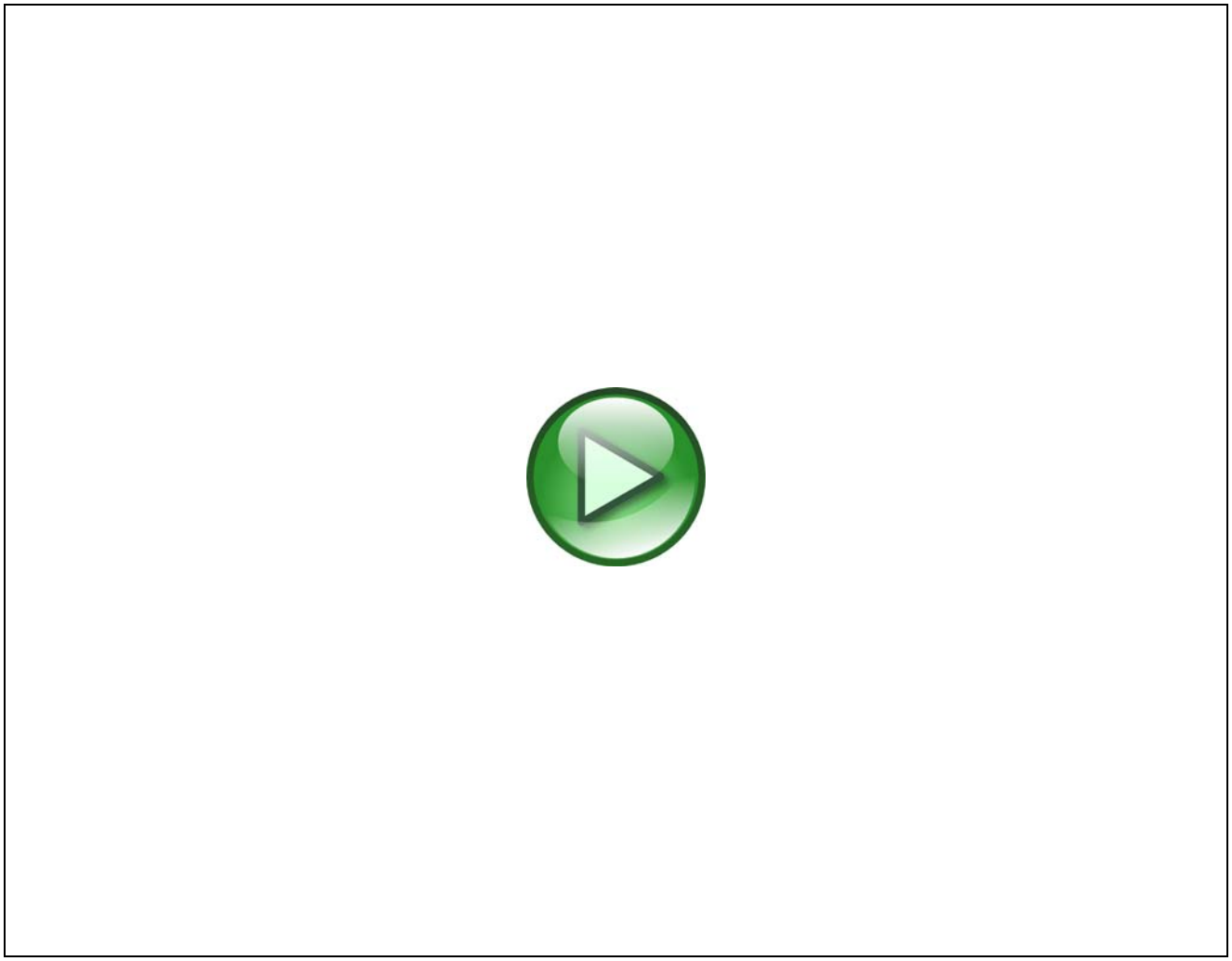
3 To access **Bob_private**, you need to enter the correct user name and password.



Once you access **Bob_private** via your ADSL Device, you do not have to relogin unless you restart your computer.

3.5.3 File Sharing Video Example

Use Adobe Reader 9 or later to play this example video. You may need to allow playback in Adobe reader and click play again to get it to start.



3.6 Using the Print Server Feature

In this section you can:

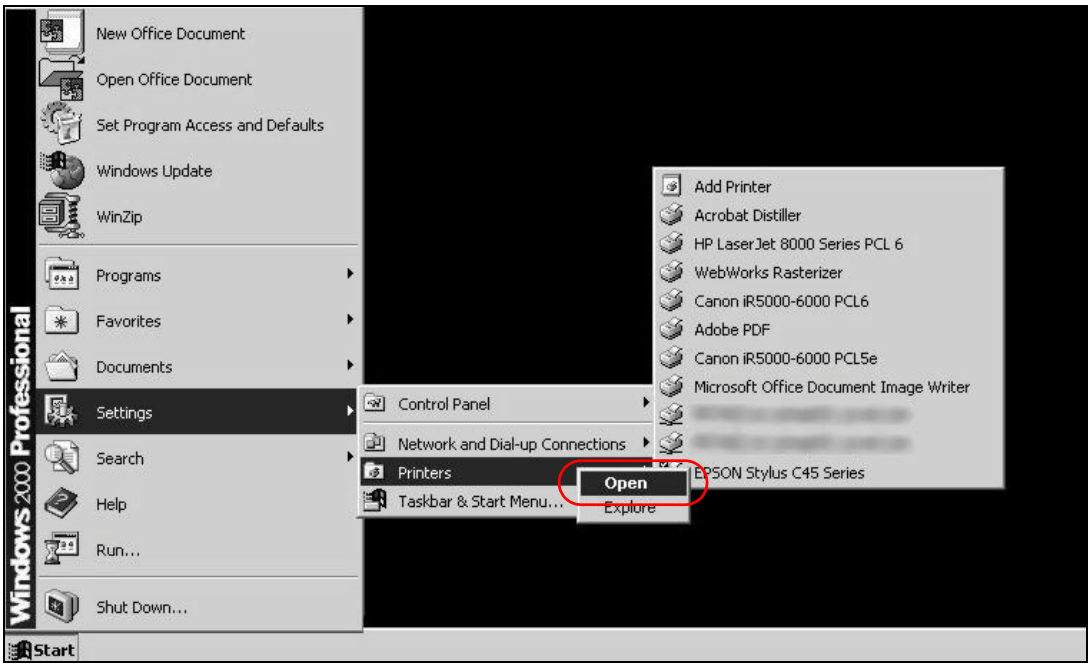
- Configure a TCP/IP Printer Port. This allows a printer connected to the ADSL Device to be used by all users in your LAN as if it was directly connected to their computers.
- Add a New Printer Using Windows
- Add a New Printer Using Macintosh OS X

Configure a TCP/IP Printer Port

This example shows how you can configure a TCP/IP printer port. This example is done using the Windows 2000 Professional operating system. Some menu items may look different on your operating system. The TCP/IP port must be configured with the IP address of the ADSL Device and must use the LPR protocol to communicate with the printer. Consult your operating systems

documentation for instructions on how to do this or follow the instructions below if you have a Windows 2000/XP operating system.

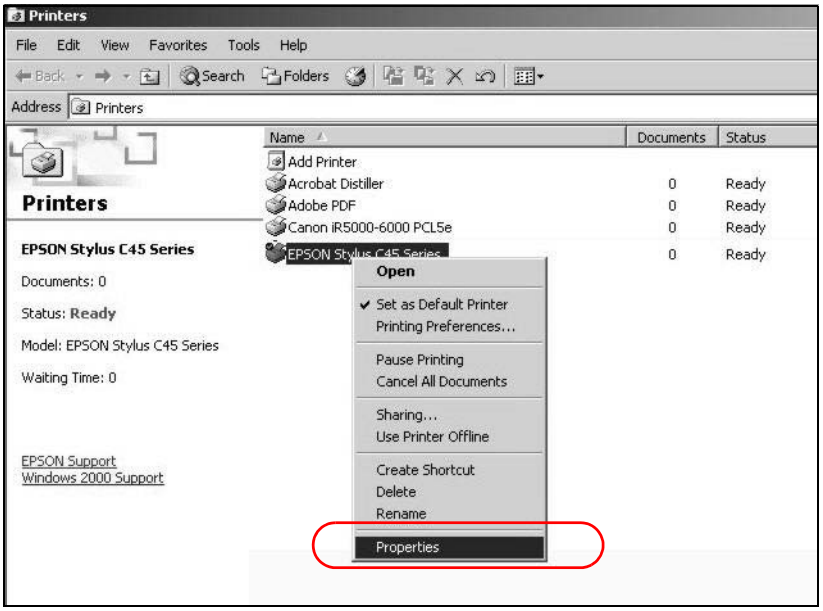
1 Click **Start** > **Settings**, then right click on **Printers** and select **Open**.



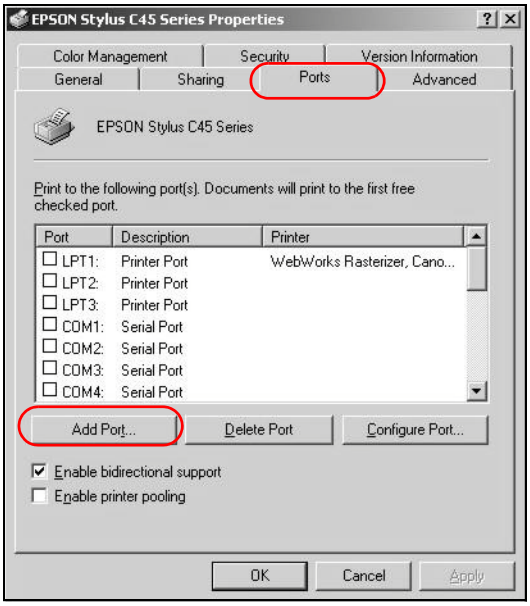
The **Printers** folder opens up. First you need to open up the properties windows for the printer you want to configure a TCP/IP port.

2 Locate your printer.

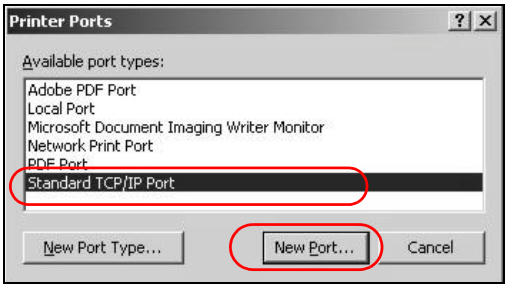
3 Right click on your printer and select **Properties**.



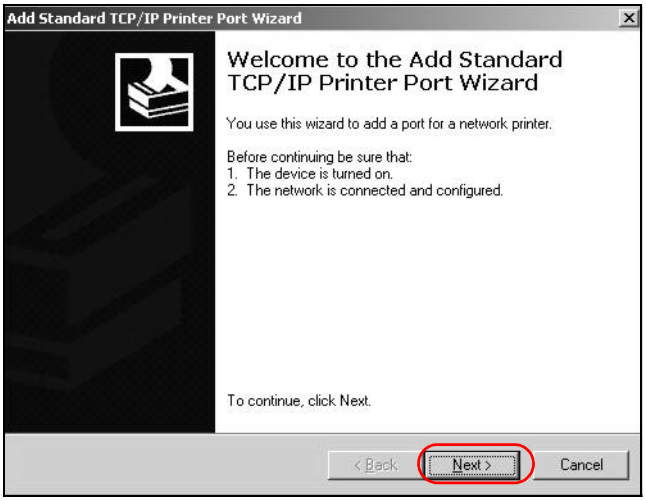
4 Select the **Ports** tab and click **Add Port...**



5 A **Printer Ports** window appears. Select **Standard TCP/IP Port** and click **New Port..**.

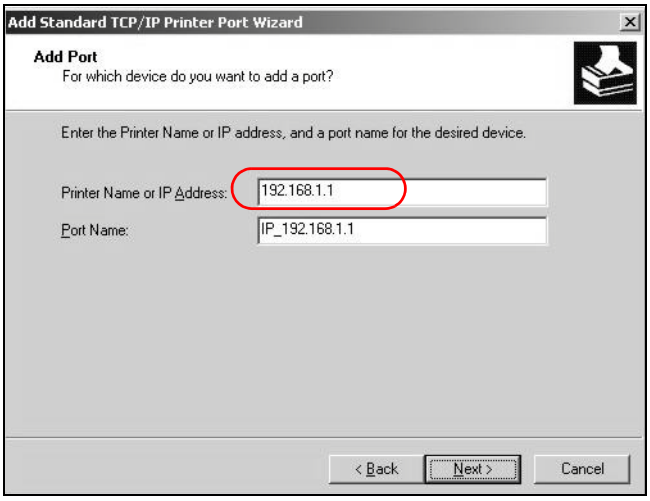


6 **Add Standard TCP/IP Printer Port Wizard** window opens up. Click **Next** to start configuring the printer port.

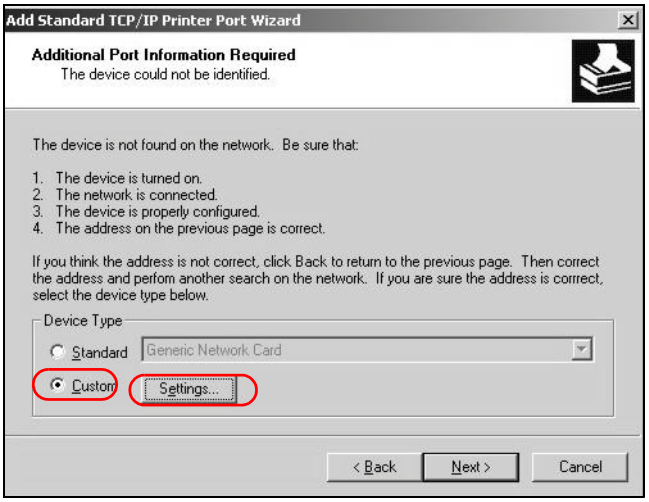

Add Standard TCP/IP Printer Port Wizard
Welcome to the Add Standard TCP/IP Printer Port Wizard
You use this wizard to add a port for a network printer.
Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.
To continue, click Next.
< Back
Next >
Cancel

7 Enter the IP address of the ADSL Device to which the printer is connected in the **Printer Name or IP Address:** field. In our example we use the default IP address of the ADSL Device, 192.168.1.1. The **Port Name** field updates automatically to reflect the IP address of the port. Click **Next**.

Note: The computer from which you are configuring the TCP/IP printer port must be on the same LAN in order to use the printer sharing function.


Add Standard TCP/IP Printer Port Wizard
Add Port
For which device do you want to add a port?
Enter the Printer Name or IP address, and a port name for the desired device.
Printer Name or IP Address:
192.168.1.1
Port Name:
IP_192.168.1.1
< Back
Next >
Cancel

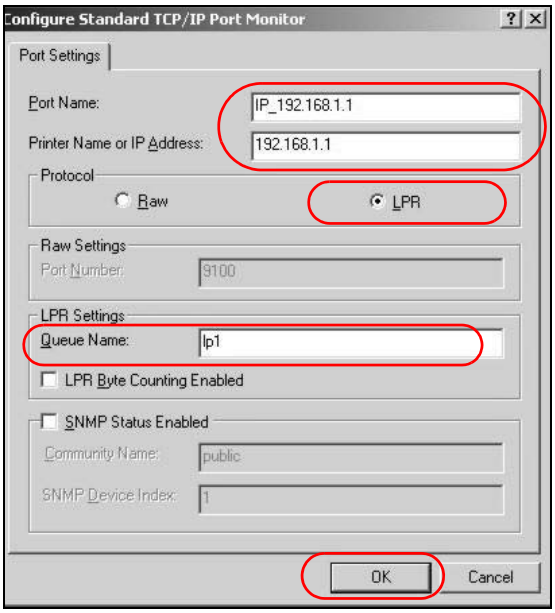
8 Select **Custom** under **Device Type** and click **Settings**.


Add Standard TCP/IP Printer Port Wizard
Additional Port Information Required
The device could not be identified.
The device is not found on the network. Be sure that:
1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perfom another search on the network. If you are sure the address is correct, select the device type below.
Device Type
Standard
Generic Network Card
Custom
Settings...
< Back
Next >
Cancel

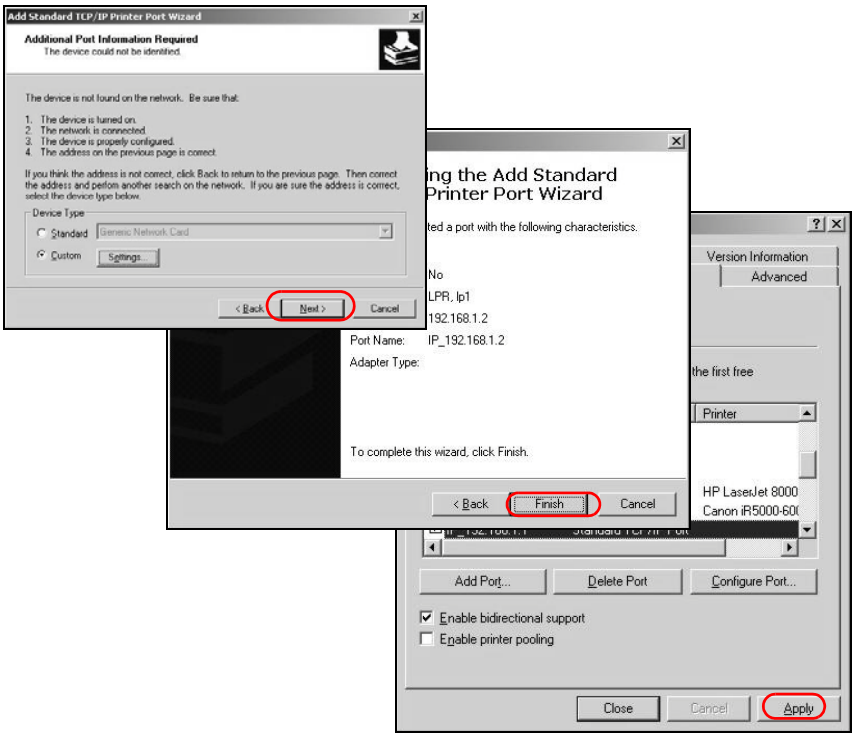
9 Confirm the IP address of the ADSL Device in the IP Address field.

10 Select **LPR** under **Protocol**.

11 Type the LPR queue name of your printer model in the **Queue Name** field and click **OK**. Refer to your printer documentation for the LPR queue name. Some printer models accept any name you want to use, in this case you can enter a short descriptive name for the **Queue Name**.



12 Continue through the wizard, apply your settings and close the wizard window.

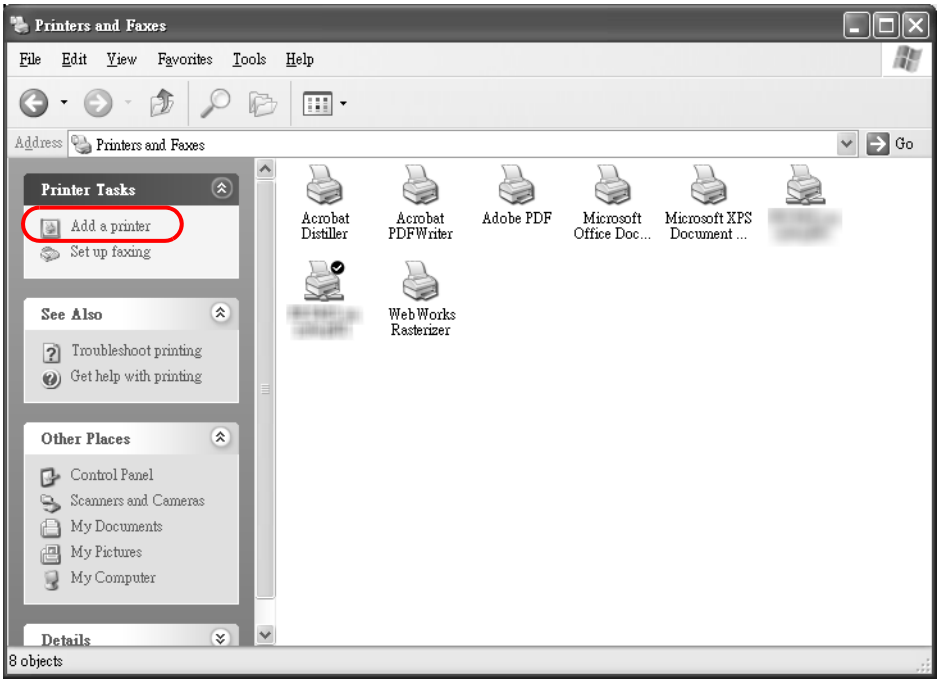

Add Standard TCP/IP Printer Port Wizard
Additional Port Information Required
The device could not be identified.
The device is not found on the network. Be sure that:
1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.
Device Type
Standard
Custom
Settings...
< Back
Next >
Cancel
ing the Add Standard Printer Port Wizard
ted a port with the following characteristics.
No
LPR, lp1
192.168.1.2
Port Name:
IP_192.168.1.2
Adapter Type:
To complete this wizard, click Finish.
< Back
Finish
Cancel
Version Information
Advanced
the first free
Printer
HP LaserJet 8000
Canon iR5000-60
Add Port...
Delete Port
Configure Port...
Enable bidirectional support
Enable printer pooling
Close
Cancel
Apply

13 Repeat steps 1 to 12 to add this printer to other computers on your network.

Add a New Printer Using Windows

This example shows how to connect a printer to your ADSL Device using the Windows XP Professional operating system. Some menu items may look different on your operating system.

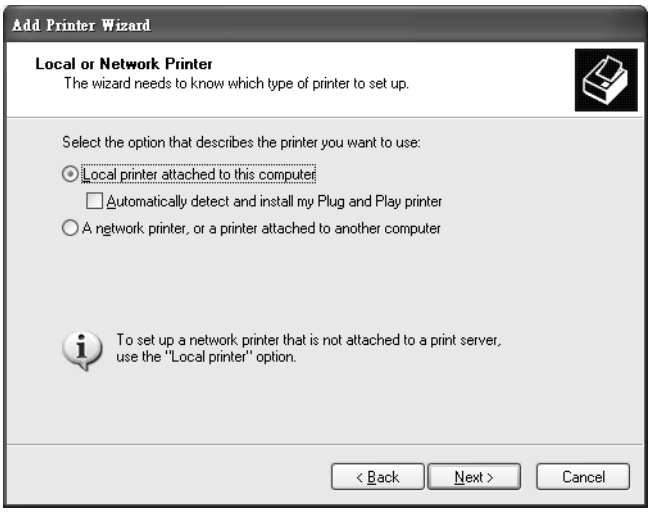
1 Click **Start** > **Control Panel** > **Printers and Faxes** to open the **Printers and Faxes** screen. Click **Add a Printer**.



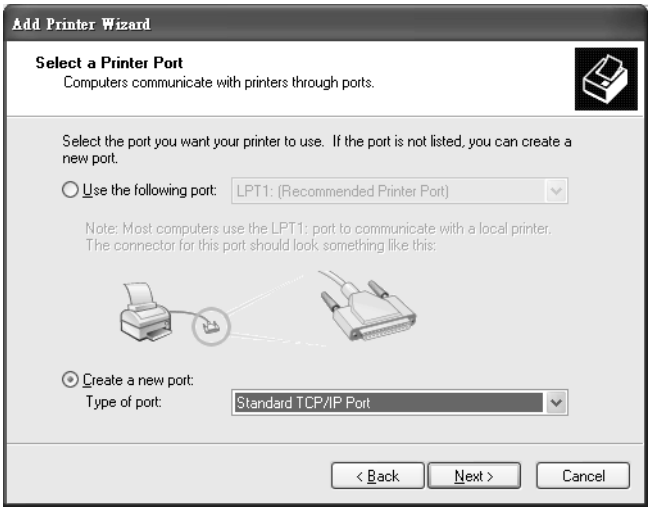
2 The **Add Printer Wizard** screen displays. Click **Next**.


Add Printer Wizard
Welcome to the Add Printer Wizard
This wizard helps you install a printer or make printer connections.
If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.
To continue, click Next.
< Back
Next >
Cancel

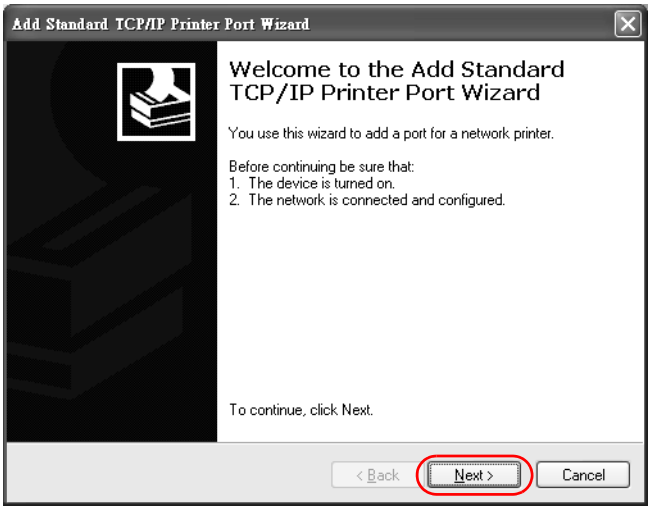
3 Select **Local printer attached to this computer** and click **Next**.


Add Printer Wizard
Local or Network Printer
The wizard needs to know which type of printer to set up.
Select the option that describes the printer you want to use:
Local printer attached to this computer
Automatically detect and install my Plug and Play printer
A network printer, or a printer attached to another computer
To set up a network printer that is not attached to a print server, use the "Local printer" option.
< Back
Next >
Cancel

4 Select **Create a new port** and **Standard TCP/IP Port**. Click **Next**.

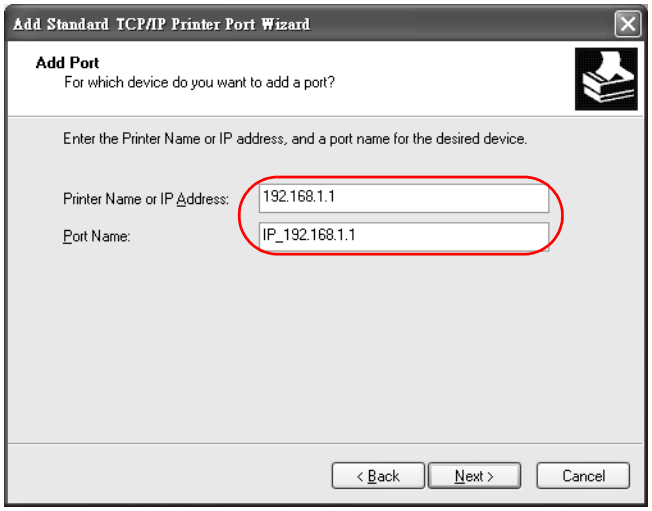

Add Printer Wizard
Select a Printer Port
Computers communicate with printers through ports.
Select the port you want your printer to use. If the port is not listed, you can create a new port.
Use the following port:
LPT1: (Recommended Printer Port)
Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:
Create a new port:
Type of port:
Standard TCP/IP Port
< Back
Next >
Cancel

5 **Add Standard TCP/IP Printer Port Wizard** window opens up. Click **Next** to start configuring the printer port.

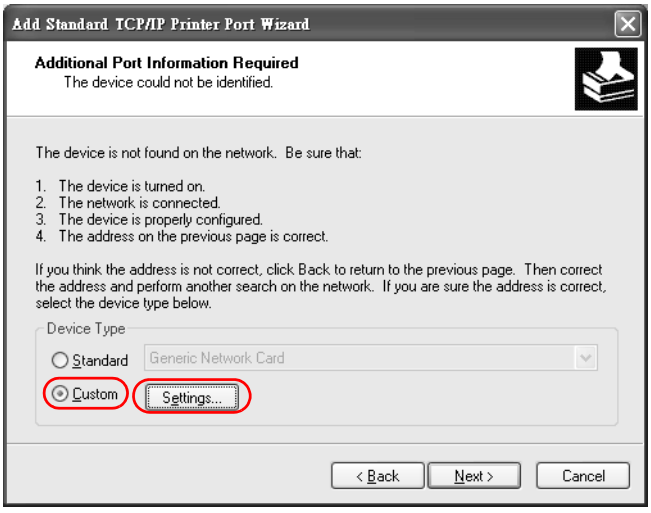

Add Standard TCP/IP Printer Port Wizard
Welcome to the Add Standard TCP/IP Printer Port Wizard
You use this wizard to add a port for a network printer.
Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.
To continue, click Next.
< Back
Next >
Cancel

6 Enter the IP address of the ADSL Device to which the printer is connected in the **Printer Name or IP Address:** field. In our example we use the default IP address of the ADSL Device, 192.168.1.1. The **Port Name** field updates automatically to reflect the IP address of the port. Click **Next**.

Note: The computer from which you are configuring the TCP/IP printer port must be on the same LAN in order to use the printer sharing function.


Add Standard TCP/IP Printer Port Wizard
Add Port
For which device do you want to add a port?
Enter the Printer Name or IP address, and a port name for the desired device.
Printer Name or IP Address:
192.168.1.1
Port Name:
IP_192.168.1.1
< Back
Next >
Cancel

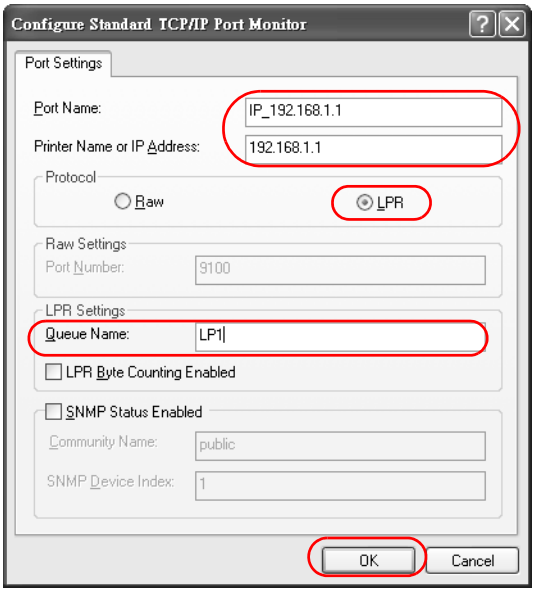
7 Select **Custom** under **Device Type** and click **Settings**.


Add Standard TCP/IP Printer Port Wizard
Additional Port Information Required
The device could not be identified.
The device is not found on the network. Be sure that:
1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.
Device Type
Standard
Generic Network Card
Custom
Settings...
< Back
Next >
Cancel

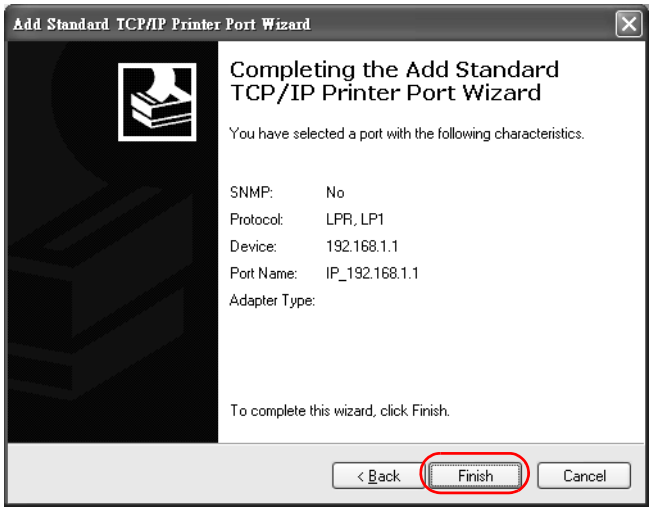
8 Confirm the IP address of the ADSL Device in the Printer **Name or IP Address** field.

9 Select **LPR** under **Protocol**.

10 Type **LP1** in the **Queue Name** field and click **OK** to go back to the previous screen and click **Next**.



11 Click **Finish** to close the wizard window.

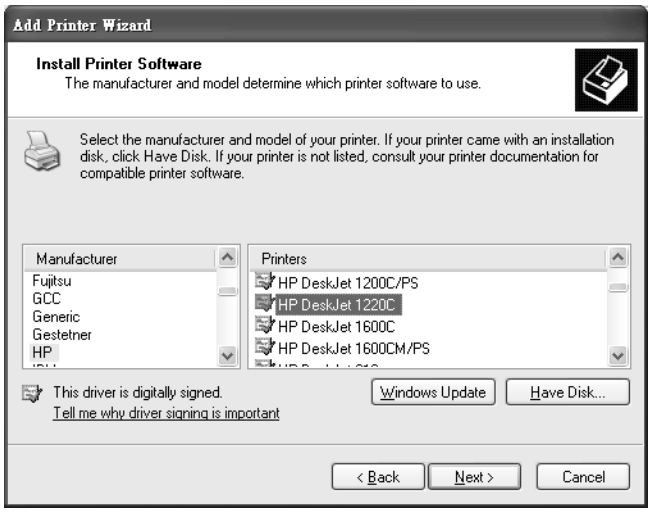


12 Select the make of the printer that you want to connect to the print server in the **Manufacturer** list of printers.

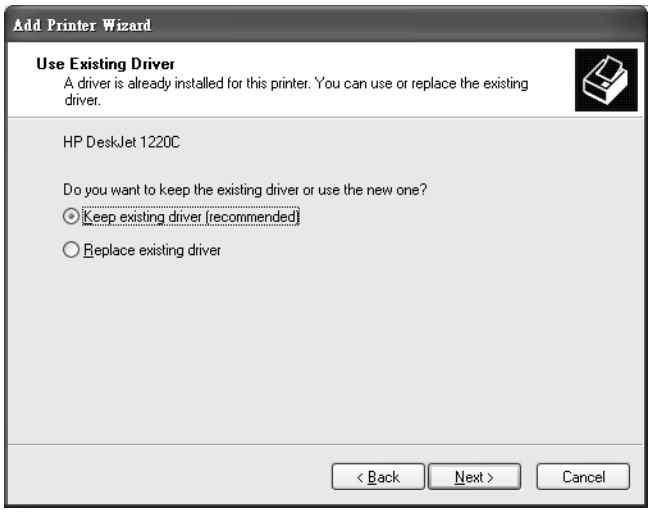
13 Select the printer model from the list of **Printers**.

14 If your printer is not displayed in the list of **Printers**, you can insert the printer driver installation CD/disk or download the driver file to your computer, click **Have Disk...** and install the new printer driver.

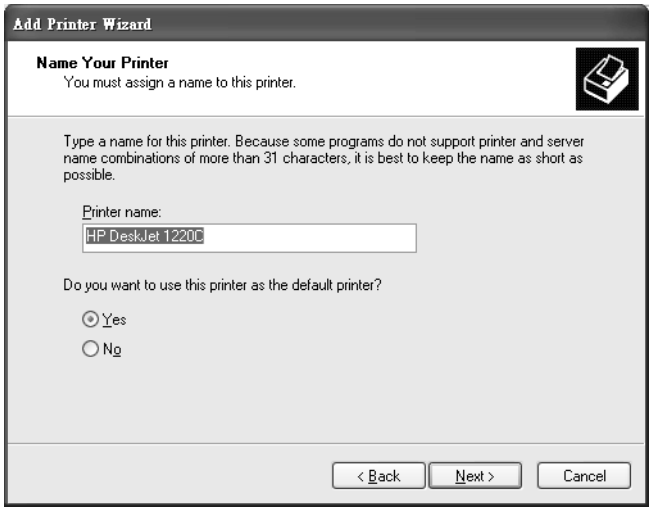
15 Click **Next** to continue.


Add Printer Wizard
Install Printer Software
The manufacturer and model determine which printer software to use.
Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.
Manufacturer
Fujitsu
GCC
Generic
Gestetner
HP
Printers
HP DeskJet 1200C/PS
HP DeskJet 1220C
HP DeskJet 1600C
HP DeskJet 1600CM/PS
This driver is digitally signed.
Tell me why driver signing is important
Windows Update
Have Disk...
< Back
Next >
Cancel

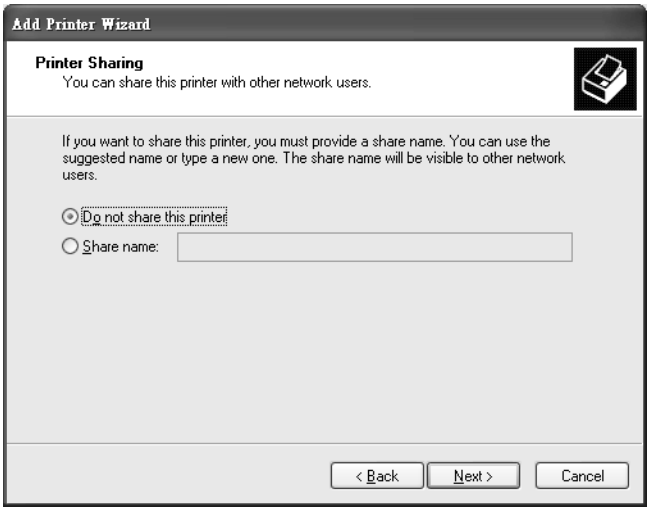
16 If the following screen displays, select **Keep existing driver** radio button and click **Next** if you already have a printer driver installed on your computer and you do not want to change it. Otherwise, select **Replace existing driver** to replace it with the new driver you selected in the previous screen and click **Next**.


Add Printer Wizard
Use Existing Driver
A driver is already installed for this printer. You can use or replace the existing driver.
HP DeskJet 1220C
Do you want to keep the existing driver or use the new one?
Keep existing driver (recommended)
Replace existing driver
< Back
Next >
Cancel

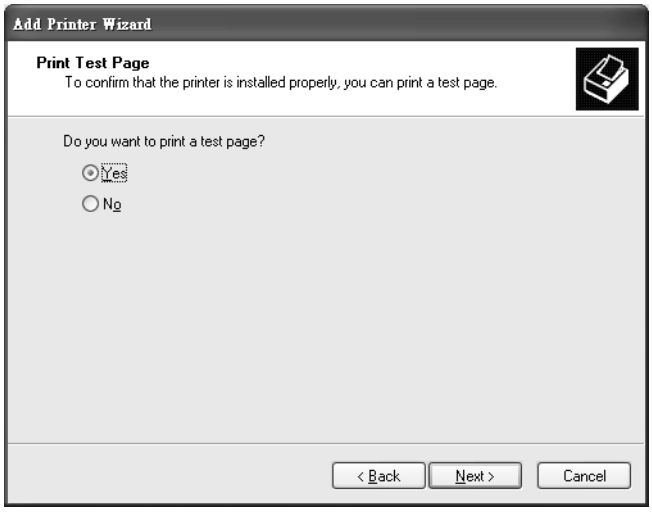
17 Type a name to identify the printer and then click **Next** to continue.


Add Printer Wizard
Name Your Printer
You must assign a name to this printer.
Type a name for this printer. Because some programs do not support printer and server name combinations of more than 31 characters, it is best to keep the name as short as possible.
Printer name:
HP DeskJet 1220C
Do you want to use this printer as the default printer?
Yes
No
< Back
Next >
Cancel

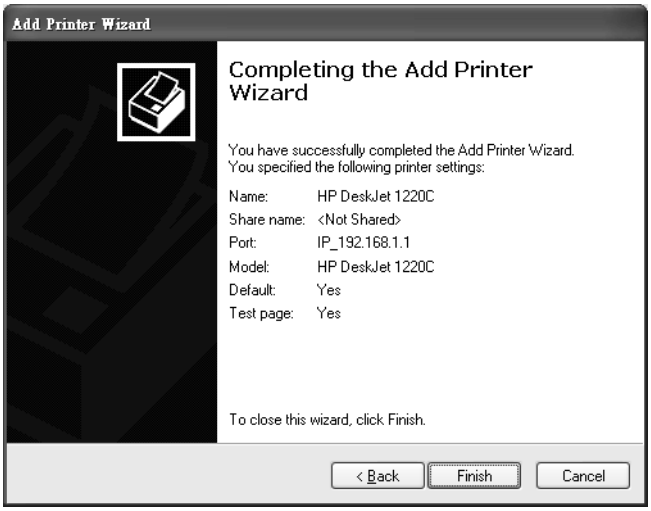
18 The ADSL Device is a print server itself and you do not need to have your computer act as a print server by sharing the printer with other users in the same network; just select **Do not share this printer** and click **Next** to proceed to the following screen.


Add Printer Wizard
Printer Sharing
You can share this printer with other network users.
If you want to share this printer, you must provide a share name. You can use the suggested name or type a new one. The share name will be visible to other network users.
Do not share this printer
Share name:
< Back
Next >
Cancel

19 Select **Yes** and then click the **Next** button if you want to print a test page. A pop-up screen displays to ask if the test page printed correctly. Otherwise select **No** and then click **Next** to continue.


Add Printer Wizard
Print Test Page
To confirm that the printer is installed properly, you can print a test page.
Do you want to print a test page?
Yes
No
< Back
Next >
Cancel

20 The following screen shows your current printer settings. Select **Finish** to complete adding a new printer.



Add a New Printer Using Macintosh OS X

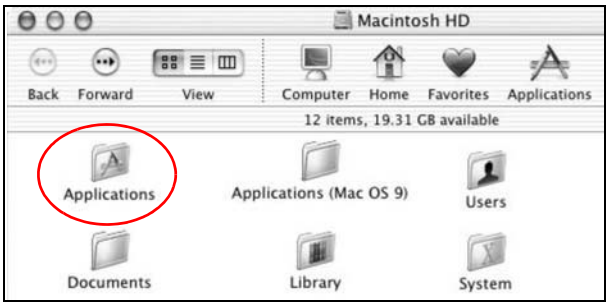
Complete the following steps to set up a print server driver on your Macintosh computer.

1 Click the **Print Center** icon  located in the Macintosh Dock (a place holding a series of icons/ shortcuts at the bottom of the desktop). Proceed to step 6 to continue. If the **Print Center** icon is not in the Macintosh Dock, proceed to the next step.

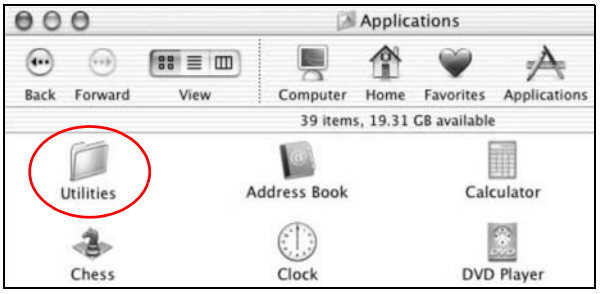
2 On your desktop, double-click the **Macintosh HD** icon to open the **Macintosh HD** window.



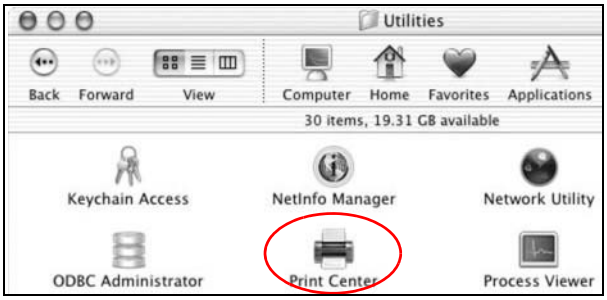
3 Double-click the **Applications** folder.



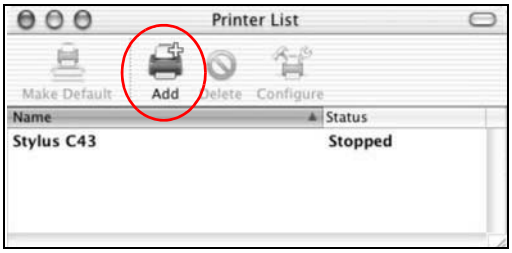
4 Double-click the **Utilities** folder.



5 Double-click the **Print Center** icon.



6 Click the **Add** icon at the top of the screen.



7 Set up your printer in the **Printer List** configuration screen. Select **IP Printing** from the drop-down list box.

8 In the **Printer's Address** field, type the IP address of your ADSL Device.

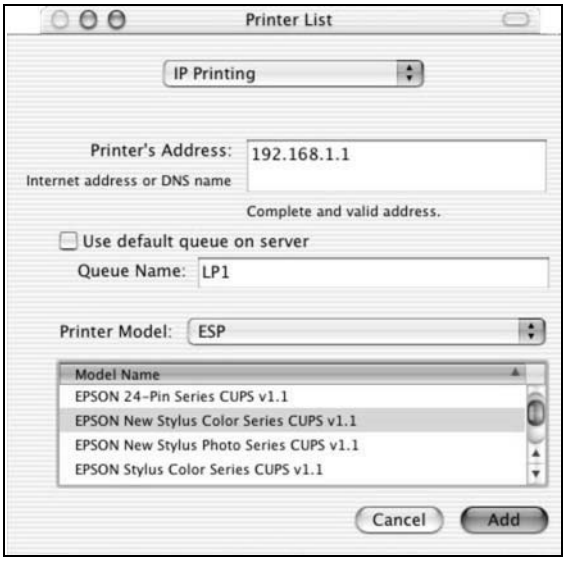
9 Deselect the **Use default queue on server** check box.

10 Type **LP1** (a parallel port) in the **Queue Name** field.

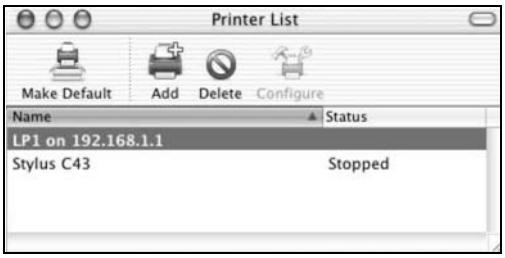
11 Select your **Printer Model** from the drop-down list box. If the printer's model is not listed, select **Generic**.



12 Click **Add** to select a printer model, save and close the **Printer List** configuration screen.



13 The **Name LP1 on 192.168.1.1** displays in the **Printer List** field. The default printer **Name** displays in bold type.

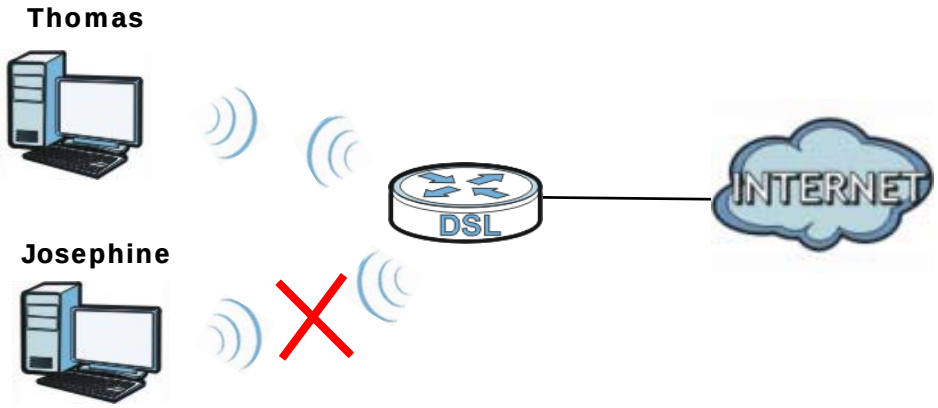


Your Macintosh print server driver setup is complete. You can now use the ADSL Device's print server to print from a Macintosh computer.

3.7 Configuring the MAC Address Filter for Restricting Wireless Internet Access

Thomas noticed that his daughter Josephine spends too much time surfing the web and downloading media files. He decided to prevent Josephine from accessing the Internet so that she can concentrate on preparing for her final exams.

Josephine's computer connects wirelessly to the Internet through the ADSL Device. Thomas decides to use the **Security > MAC Filter** screen to grant wireless network access to his computer but not to Josephine's computer.



1 Thomas should check the wireless card's MAC address on his computer first. For example, open **Command Prompt** and use the "ipconfig /all" command on Windows. The Physical Address (**00:60:B3:00:B5:EB**) indicates the wireless card's MAC address.

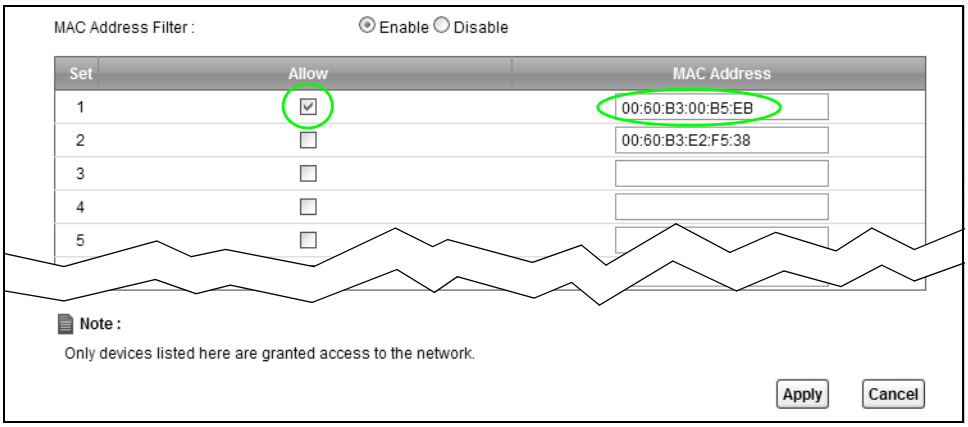
```
C:\Documents and Settings\mt01275>ipconfig /all

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . : P-660HNU-F1
        Description . . . . . . . . . . . : ZyXEL G-220 v2 Wireless USB Adapter
        Physical Address. . . . . . . . . : 00-60-B3-00-B5-EB
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.44
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 192.168.1.1
        Lease Obtained. . . . . . . . . . : Tuesday, December 13, 2011 13:28:22
        Lease Expires . . . . . . . . . . : Wednesday, December 14, 2011 13:28:22
```

2 Click **Security** > **MAC Filter** to open the **MAC Filter** screen. Select the **Enable** check box to activate MAC filter function.

3 The ADSL Device automatically adds all connected net cards' MAC addresses to the table in this screen. Find the MAC address of Thomas' computer in this screen. Select **Allow**. Click **Apply**.

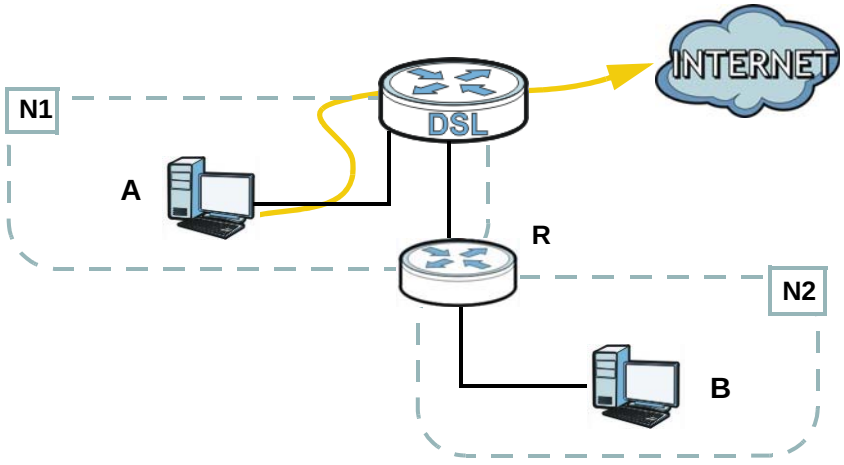


Thomas can also grant access to the computers of other members of his family and friends. However, Josephine and others not listed in this screen will no longer be able to access the Internet through the ADSL Device.

3.8 Configuring Static Route for Routing to Another Network

In order to extend your Intranet and control traffic flowing directions, you may connect a router to the ADSL Device's LAN. The router may be used to separate two department networks. This tutorial shows how to configure a static routing rule for two network routings.

In the following figure, router **R** is connected to the ADSL Device's LAN. **R** connects to two networks, **N1** (192.168.1.x/24) and **N2** (192.168.10.x/24). If you want to send traffic from computer **A** (in **N1** network) to computer **B** (in **N2** network), the traffic is sent to the ADSL Device's WAN default gateway by default. In this case, **B** will never receive the traffic.



You need to specify a static routing rule on the ADSL Device to specify **R** as the router in charge of forwarding traffic to **N2**. In this case, the ADSL Device routes traffic from **A** to **R** and then **R** routes the traffic to **B**.This tutorial uses the following example IP settings:

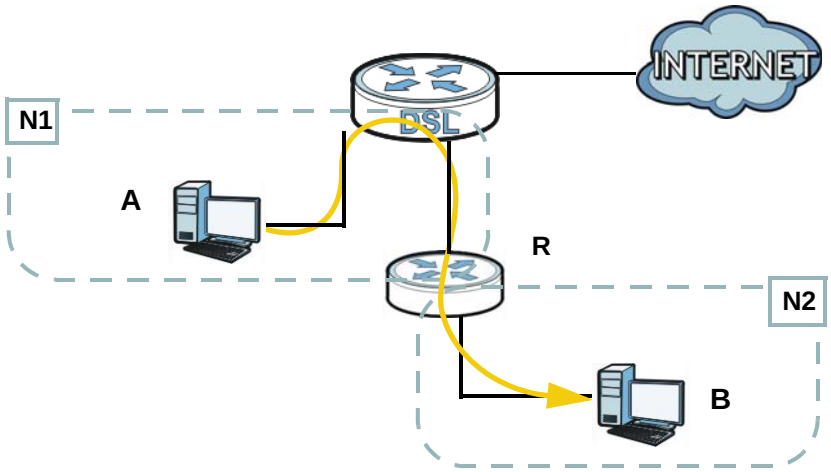
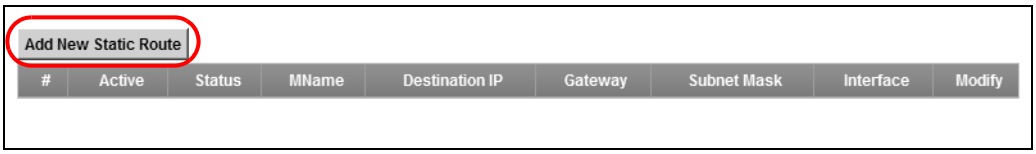


Table 8 IP Settings in this Tutorial

DEVICE / COMPUTER	IP ADDRESS
The ADSL Device's WAN	172.16.1.1
The ADSL Device's LAN	192.168.1.1
A	192.168.1.34
R's N1	192.168.1.253
R's N2	192.168.10.2
B	192.168.10.33

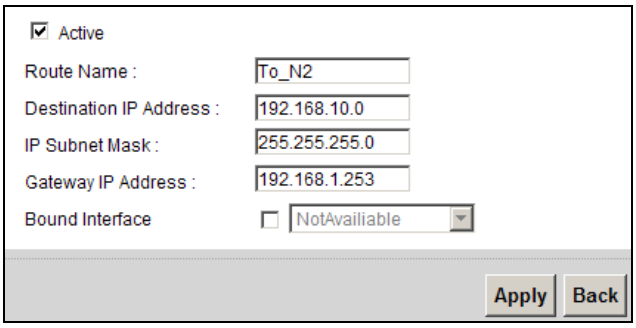
To configure a static route to route traffic from **N1** to **N2**:

1 Click **Network Setting > Static Route**. Click **Add New Static Route**.

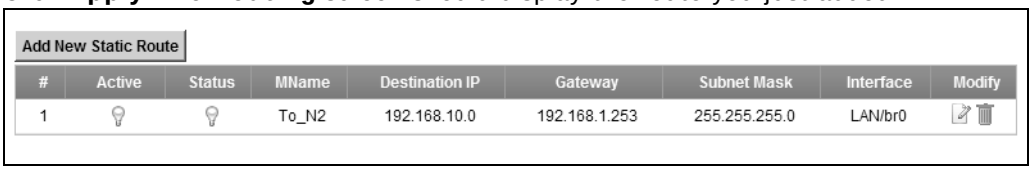


2 Configure the **Static Route Setup** screen using the following settings:

- Select **Active**.
- Specify a descriptive name for this routing rule.
- Type **192.168.10.0** and subnet mask **255.255.255.0** for the destination, **N2**.
- Type **192.168.1.253** (**R**'s N1 address) in the **Gateway IP Address** field.



Click **Apply**. The **Routing** screen should display the route you just added.


Add New Static Route
Active Status MName Destination IP Gateway Subnet Mask Interface Modify
1 To_N2 192.168.10.0 192.168.1.253 255.255.255.0 LAN/br0

Now **B** should be able to receive traffic from **A**. You may need to additionally configure **B**'s firewall settings to allow specific traffic to pass through.

3.9 Configuring QoS Queue and Class Setup

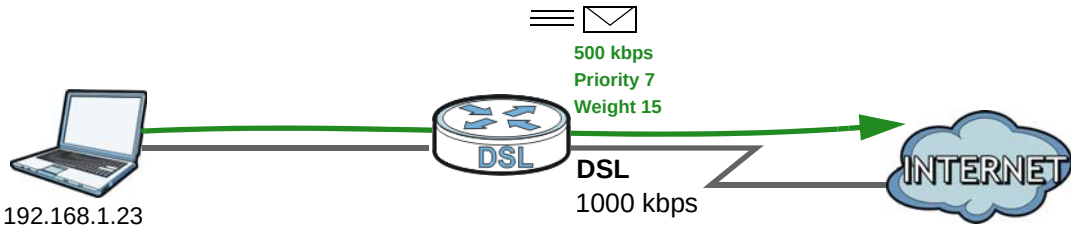
This section contains tutorials on how you can configure the QoS screen.

Note: Voice traffic will not be affected by the user-defined QoS settings on the ADSL Device. It always gets the highest priority.

This example assumes that you want to prioritize e-mail traffic because you have to send important mails and urgent updates to clients very often.

In the following figure, your Internet connection has an upstream transmission bandwidth of 1000 kbps. For this example, you want to configure QoS so that e-mail traffic gets the highest priority with at least 500 kbps. You can do the following:

- Configure a queue to assign the highest priority queue (7) to e-mail traffic sent from the LAN interface, so that e-mail traffic would not get delayed when there is network congestion.
- Note the IP address (192.168.1.23 for example) and/or MAC address (AA:FF:AA:FF:AA:FF for example) of your computer and map them to queue 7.

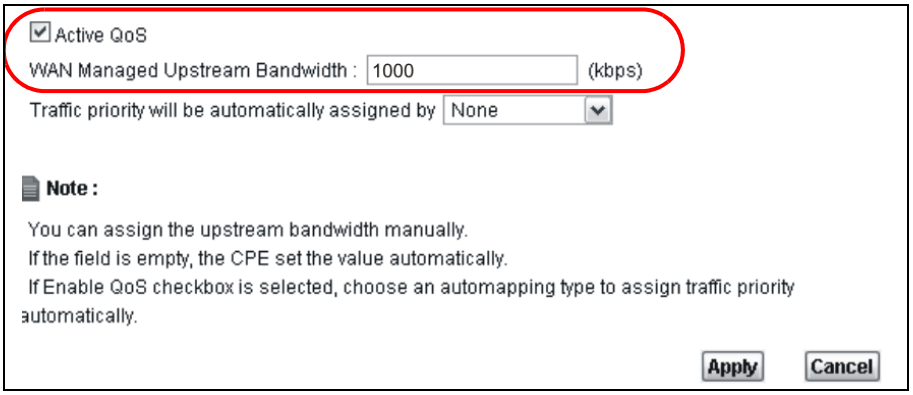


QoS allows the ADSL Device to group and prioritize application traffic and fine-tune network performance. The ADSL Device assigns each packet a priority and queues the packet according to your configured classifiers. Classifiers define how to sort traffic into different flows, assign priority, and define actions to be performed for classified traffic flows.

Note: QoS is applied to traffic flowing out of the ADSL Device.

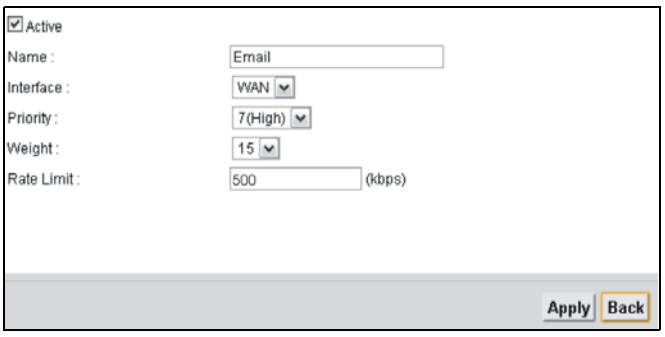
Traffic that does not match this class is assigned a priority queue based on the internal QoS mapping table on the ADSL Device.

1 Click **Network Setting > QoS > General** and check **Active**. Set your **WAN Managed Upstream Bandwidth** to 1000 kbps (or leave this blank to have the ADSL Device automatically determine this figure). Click **Apply** to save your settings.

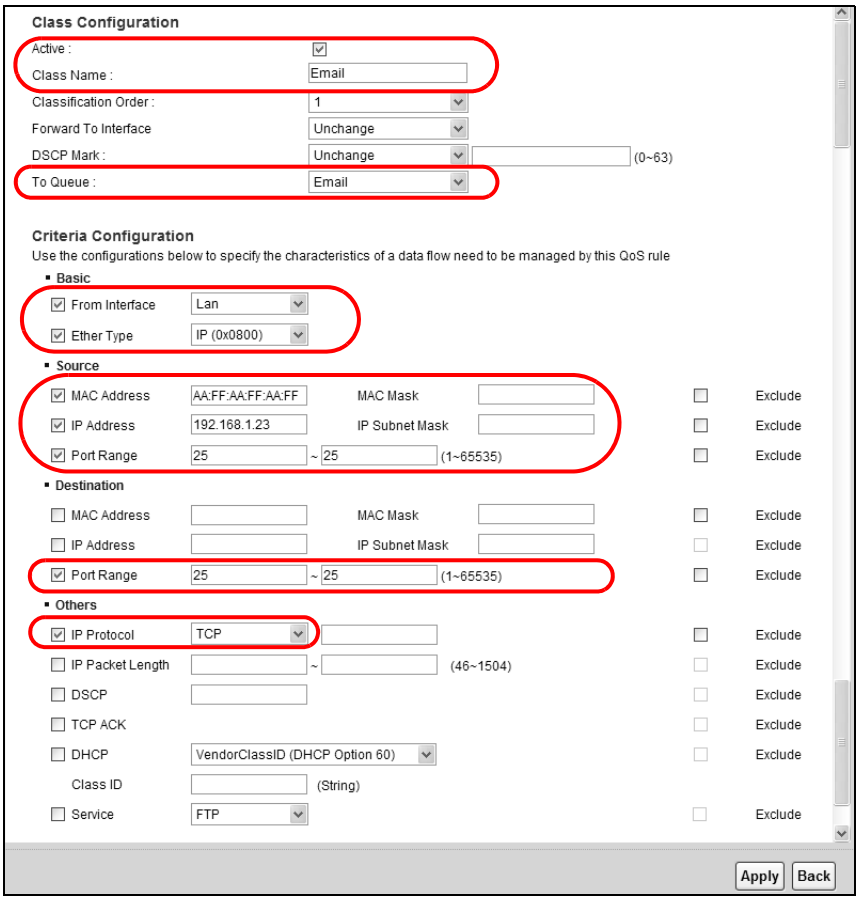

Active QoS
WAN Managed Upstream Bandwidth : 1000 (kbps)
Traffic priority will be automatically assigned by None
Note :
You can assign the upstream bandwidth manually.
If the field is empty, the CPE set the value automatically.
If Enable QoS checkbox is selected, choose an automapping type to assign traffic priority automatically.
Apply
Cancel

2 Go to **Network Setting > QoS > Queue Setup**. Click **Add new Queue** to create a new queue. In the screen that opens, check **Active** and enter or select the following values, then click **Apply**.

- **Name**: Email
- **Priority**: 7 (High)
- **Weight**: 15
- **Rate Limit**: 500 (kbps)



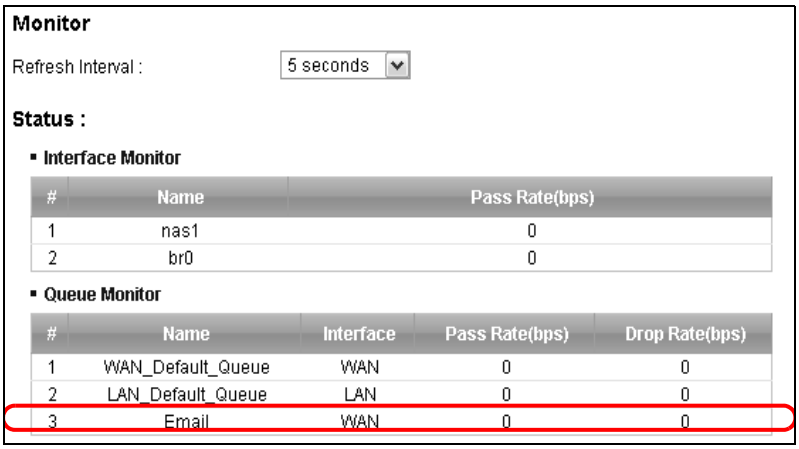
3 Go to **Network Setting > QoS > Class Setup**. Click **Add new Classifier** to create a new class. Check **Active** and follow the settings as shown in the screen below. Then click **Apply**.


Class Configuration
Active :
Class Name : Email
Classification Order : 1
Forward To Interface : Unchange
DSCP Mark : Unchange (0~63)
To Queue : Email
Criteria Configuration
Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule
Basic
From Interface : Lan
Ether Type : IP (0x0800)
Source
MAC Address : AA:FF:AA:FF:AA:FF MAC Mask Exclude
IP Address : 192.168.1.23 IP Subnet Mask Exclude
Port Range : 25 ~ 25 (1~65535) Exclude
Destination
MAC Address MAC Mask Exclude
IP Address IP Subnet Mask Exclude
Port Range : 25 ~ 25 (1~65535) Exclude
Others
IP Protocol : TCP Exclude
IP Packet Length ~ (46~1504) Exclude
DSCP Exclude
TCP ACK Exclude
DHCP : VendorClassID (DHCP Option 60) Exclude
Class ID (String)
Service : FTP Exclude
Apply
Back

Class Name	Give a class name to this traffic, such as **Email** in this example.
To Queue	Link this to a queue created in the **QoS > Queue Setup** screen, which is the **Email** queue created in this example.
From Interface	This is the interface from which the traffic will be coming from. Select **Lan**.
Ether Type	Select **IP** to identify the traffic source by its IP address or MAC address.
Source - MAC Address	Type the MAC address of your computer - **AA:FF:AA:FF:AA:FF**. Type the **MAC Mask** if you know it.
Source - IP Address	Type the IP address of your computer - **192.168.1.23**. Type the **IP Subnet Mask** if you know it.
Source - Port Range	Set the port range to **25 ~ 25**.
Destination - Port Range	Set the port range to **25 ~ 25**.
IP Protocol	Select this to make the source and destination **Port Range** fields available. Set the protocol to **TCP**.

This maps e-mail traffic to queue 7 created in the previous screen (see the **To Queue** field). This also maps your computer's IP address and MAC address to queue 7 (see the **Source** fields).

4 Verify that the queue setup works by checking **Network Setting > QoS > Monitor**. This shows the bandwidth allotted to e-mail traffic compared to other network traffic.



3.9.1 QoS Video Example

Use Adobe Reader 9 or later to play this example video. You may need to allow playback in Adobe reader and click play again to get it to start.



3.10 Access the ADSL Device Using DDNS

If you connect your ADSL Device to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The ADSL Device's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the ADSL Device using a domain name.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial shows you how to:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your ADSL Device
- Testing the DDNS Setting

Note: If you have a private WAN IP address, then you cannot use DDNS.

3.10.1 Registering a DDNS Account on www.dyndns.org

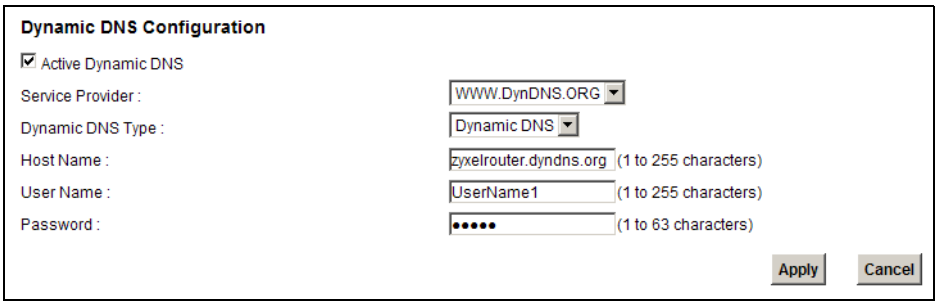
1. Open a browser and type **http://www.dyndns.org**.
2. Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.
3. Log into www.dyndns.org using your account.
4. Add a new DDNS host name. This tutorial uses the following settings as an example.
   - Host name: **zyxelrouter.dyndns.org**
   - Service Type: **Host with IP address**
   - IP Address: Enter the WAN IP address that your ADSL Device is currently using. You can find the IP address on the ADSL Device's web configurator **Status** page.

Then you will need to configure the same account and host name on the ADSL Device later.

3.10.2 Configuring DDNS on Your ADSL Device

Configure the following settings in the **Network Setting** > **DNS** screen.

- Select **Active Dynamic DNS**.
- Select **Dynamic DNS** for the Dynamic DNS type.
- Type **zyxelrouter.dyndns.org** in the **Host Name** field.
- Enter the user name (**UserName1**) and password (**12345**).



Click **Apply**.

3.10.3 Testing the DDNS Setting

Now you should be able to access the ADSL Device from the Internet. To test this:

1. Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.
2. Type **http://zyxelrouter.dyndns.org** and press [Enter].
3. The ADSL Device's login page should appear. You can then log into the ADSL Device and manage it.

PART II
Technical Reference

4

Connection Status and System Info Screens

4.1 Overview

After you log into the web configurator, the **Connection Status** screen appears. This shows the network connection status of the ZyXEL Device and clients connected to it.

Use the **System Info** screen to look at the current status of the device, system resources and interfaces (LAN, WAN, WLAN).

4.2 The Connection Status Screen

Use this screen to view the network connection status of the device and its clients. A warning message appears if there is a connection problem.

If you prefer to view the status in a list, click **List View** in the **Viewing mode** selection box. You can configure how often you want the ZyXEL Device to update this screen in **Refresh Interval**.

Figure 18 Connection Status: Icon View

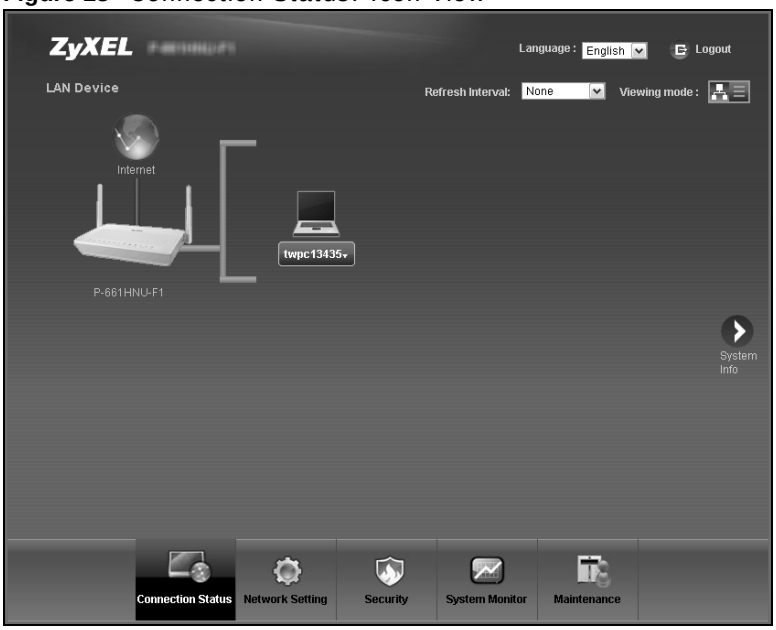
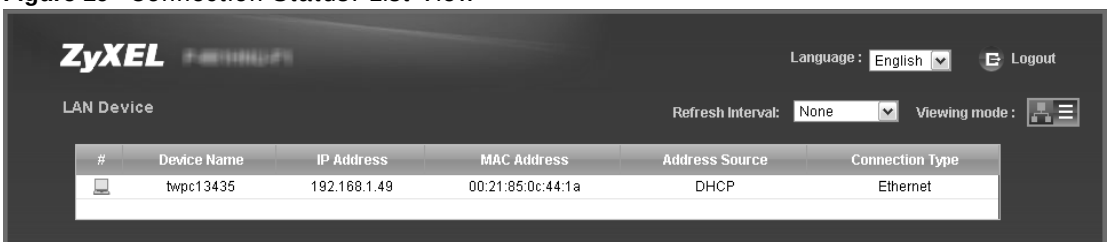


Figure 19 Connection Status: List View



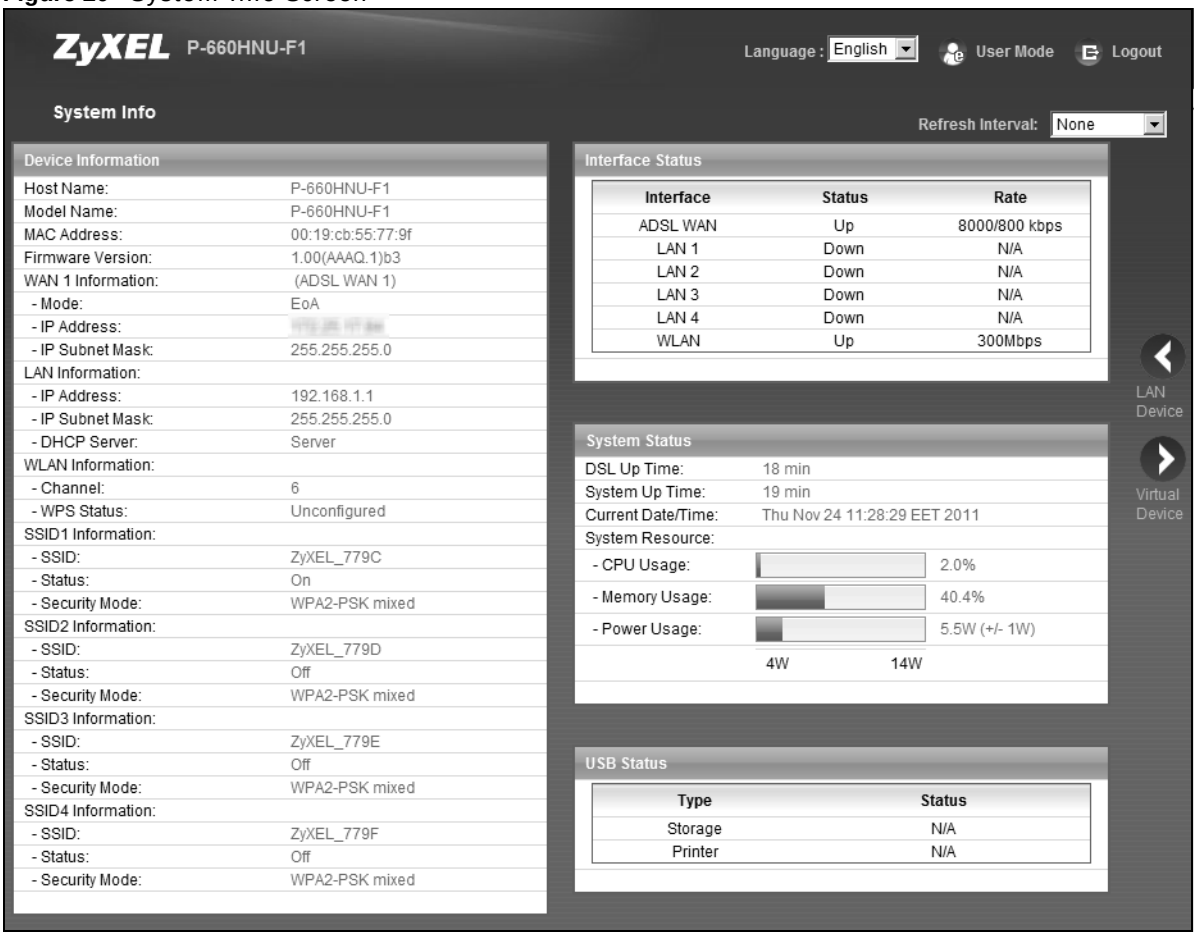
In **Icon View**, if you want to view information about a client, click the client's name and then click on **Info**. If you want to change the name or icon of the client, click the client's name and then click on **Change name/icon**.

In **List View**, you can also view the client's information.

4.3 The System Info Screen

Click **Connection Status > System Info** to open this screen.

Figure 20 System Info Screen



Each field is described in the following table.

Table 9 System Info Screen

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the ZyXEL Device to update this screen from the drop-down list box.
Device Information	
Host Name	This field displays the ZyXEL Device system name. It is used for identification. You can change this in the **Maintenance > System** screen's **Host Name** field.
Model Name	This is the model name of your device.
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your ZyXEL Device.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. Go to the **Maintenance > Firmware Upgrade** screen to change it.
WAN Information	
Mode	This is the method of encapsulation used by your ISP.
IP Address	This field displays the current IP address of the ZyXEL Device in the WAN.
IP Subnet Mask	This field displays the current subnet mask in the WAN.
LAN Information	
IP Address	This field displays the current IP address of the ZyXEL Device in the LAN.
IP Subnet Mask	This field displays the current subnet mask in the LAN.
DHCP Server	This field displays what DHCP services the ZyXEL Device is providing to the LAN. Choices are: **Server** - The ZyXEL Device is a DHCP server in the LAN. It assigns IP addresses to other computers in the LAN. **None** - The ZyXEL Device is not providing any DHCP services to the LAN.
WLAN Information	
Channel	This is the channel number used by the ZyXEL Device now.
WPS Status	**Configured** displays when the WPS security settings have been configured and wireless clients can connect with the device through WPS. **Unconfigured** displays when the device has not been configured and wireless clients can't establish a link with the device through WPS.
SSID (1~4) Information	
SSID	This is the descriptive name used to identify the ZyXEL Device in the wireless LAN.
Status	This shows whether or not the SSID is enabled (on).
Security Mode	This displays the type of security the ZyXEL Device is using in the wireless LAN.
Interface Status	
Interface	This column displays each interface the ZyXEL Device has.

LABEL	DESCRIPTION
Status	This field indicates whether or not the ZyXEL Device is using the interface. For the DSL interface, this field displays **Down** (line is down), **Up** (line is up or connected), **Initializing** (line is initializing), **Establishing Link** (line is establishing a link) if you're using Ethernet encapsulation and **Down** (line is down), **Up** (line is up or connected), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation. For the LAN interface, this field displays **Up** when the ZyXEL Device is connected through an Ethernet cable to a computer or a HUB. It displays **Down** when the ZyXEL Device's Ethernet port is disconnected. For the WLAN interface, it displays **Active** when WLAN is enabled or **InActive** when WLAN is disabled.
Rate	For the LAN interface, this displays the port speed. For the WAN interface, this displays the DSL link rate downstream and upstream. For the DSL interface, it displays the downstream and upstream transmission rate. For the WLAN interface, it displays the maximum transmission rate when WLAN is enabled or **N/A** when WLAN is disabled.
System Status	
DSL Up Time	This field displays how long the DSL connection has been active
System Up Time	This field displays how long the ZyXEL Device has been running since it last started up. The ZyXEL Device starts up when you plug it in, when you restart it (**Maintenance > Reboot**), or when you reset it (see Chapter 1 on page 25).
Current Date/ Time	This field displays the current date and time in the ZyXEL Device. You can change this in **Maintenance > Time Setting**.
System Resource	
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently used. When this percentage is close to 100%, the ZyXEL Device is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications.
Memory Usage	This field displays what percentage of the ZyXEL Device's memory is currently used. Usually, this percentage should not increase much. If memory usage does get close to 100% and remains like that for a high period of time, the ZyXEL Device may become unstable and you should restart it. See Chapter 24 on page 241, or turn off the device (unplug the power) for a few seconds.
Power Usage	This field displays the electric power the device is using.
USB Status	
Type	This shows the type of device connected to the ZyXEL Device.
Status	This field shows **Available** if the USB device is currently active. It shows **N/A** if there are no device connected to the ZyXEL Device or the connected device is not working.

5

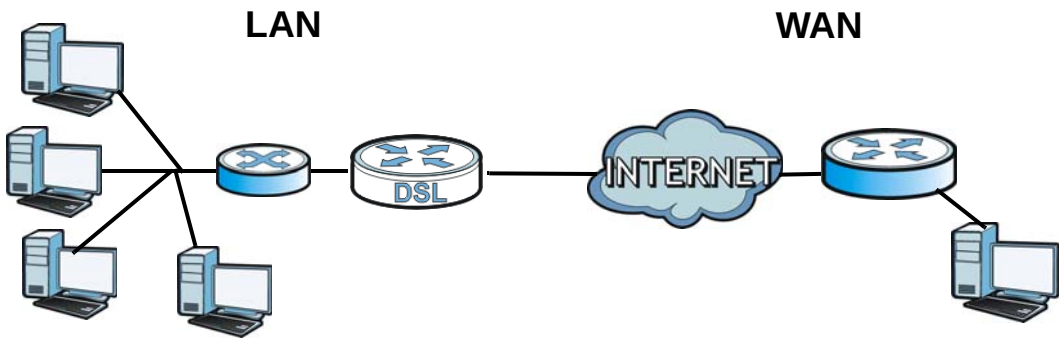
Broadband

5.1 Overview

This chapter discusses the ZyXEL Device's **Broadband** screens. Use these screens to configure your ZyXEL Device for Internet access.

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private networks, such as a LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

Figure 21 LAN and WAN



5.1.1 What You Can Do in this Chapter

- Use the **Broadband** screen to view, remove or add a WAN interface. You can also configure the WAN settings on the ZyXEL Device for Internet access (Section 5.2 on page 88).

5.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the ZyXEL Device, which makes it accessible from an outside network. It is used by the ZyXEL Device to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the ZyXEL Device tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es).

ATM

Asynchronous Transfer Mode (ATM) is a LAN and WAN networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. ATM uses a connection-oriented model and establishes a virtual circuit (VC) between two endpoints before the actual data exchange begins.

Finding Out More

- See Section 5.3 on page 100 for advanced technical information on WAN.
- See Chapter 3 on page 41 for WAN tutorials.

5.1.3 Before You Begin

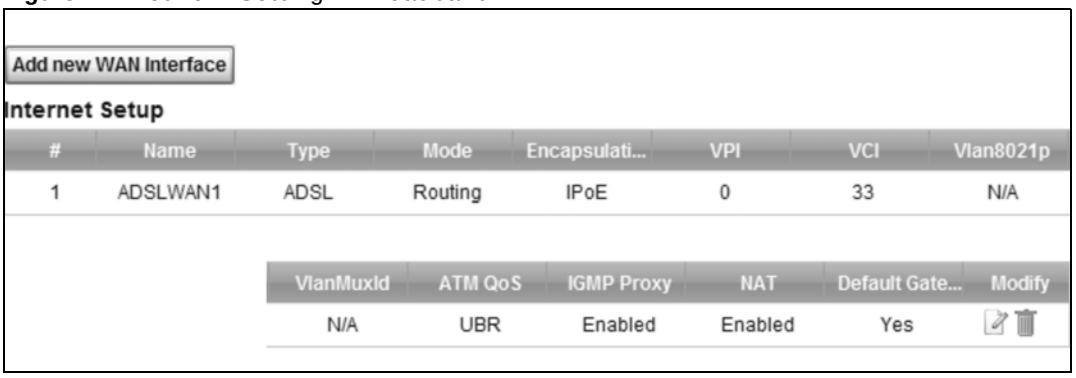
You need to know your Internet access settings such as encapsulation and WAN IP address. Get this information from your ISP.

5.2 The Broadband Screen

The ZyXEL Device must have a WAN interface to allow users to use the DSL port to access the Internet. Use the **Broadband** screen to view, remove or add a WAN interface.

Click **Network Setting > Broadband**. The following screen opens.

Figure 22 Network Setting > Broadband


Add new WAN Interface
Internet Setup
Name Type Mode Encapsulati... VPI VCI Vlan8021p
1 ADSLWAN1 ADSL Routing IPoE 0 33 N/A
VlanMuxId ATM QoS IGMP Proxy NAT Default Gate... Modify
N/A UBR Enabled Enabled Yes

The following table describes the fields in this screen.

Table 10 Network Setting > Broadband

LABEL	DESCRIPTION
Add new WAN Interface	Click this to create a new WAN interface.
Internet Setup	
#	This is the index number of the connection.
Name	This is the service name of the connection.
Type	This shows the type of interface used by this connection.
Mode	This shows whether the connection is in routing mode or bridge mode.
Encapsulation	This shows the method of encapsulation used by this connection.
VPI	This is the Virtual Path Identifier (VPI).
VCI	This is the Virtual Channel Identifier (VCI).
Vlan8021p	This indicates the 802.1P priority level assigned to traffic sent through this connection. This displays **N/A** when there is no priority level assigned.
VlanMuxId	This indicates the VLAN ID number assigned to traffic sent through this connection. This displays **N/A** when there is no VLAN ID number assigned.
ATM QoS	This shows the ATM Quality of Service (QoS) type configured for this connection. This displays **N/A** when there is no ATM QoS assigned.
IGMP Proxy	This shows whether IGMP (Internet Group Multicast Protocol) is activated or not for this connection.
NAT	This shows whether NAT is activated or not for this connection. NAT is not available when the connection uses the bridging service.
Default Gateway	This shows whether the ZyXEL Device uses the interface of this connection as the system default gateway.
Modify	Click the **Edit** icon to configure the connection. Click the **Delete** icon to delete this connection from the ZyXEL Device. A window displays asking you to confirm that you want to delete the connection.

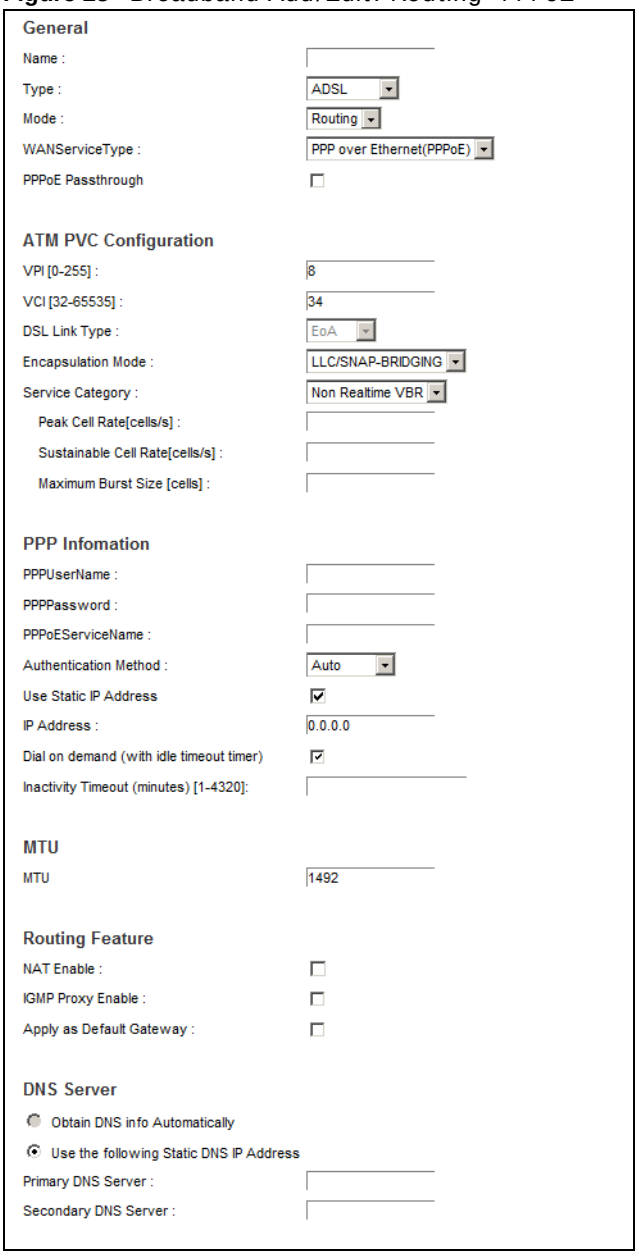
5.2.1 Add/Edit Internet Connection

Use this screen to configure a WAN connection. The screen varies depending on the encapsulation method used and WAN service type you select.

5.2.1.1 Routing- PPPoE

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **Routing** as the encapsulation mode and **PPPoE** as the WAN service type.

Figure 23 Broadband Add/Edit: Routing- PPPoE



The following table describes the fields in this screen.

Table 11 Broadband Add/Edit: Routing- PPPoE

Label	**DESCRIPTION**
General	
Name	Enter a service name of the connection.
Type	**ADSL**: The ZyXEL Device uses the ADSL technology for data transmission over the DSL port.
Mode	Select **Routing** (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account.

Table 11 Broadband Add/Edit: Routing- PPPoE (continued)

Label	DESCRIPTION
WAN Service Type	This field is available only when you select **Routing** in the **Mode** field. Select the method of encapsulation used by your ISP. • **PPP over Ethernet (PPPoE)** - PPPoE (Point to Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. Select this if you have a username and password for Internet access. • **IP over Ethernet** - In this type of Internet connection, IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. • **PPP over ATM** - PPPoA offers standard PPP features, such as authentication, encryption, and compression. It is used as the connection encapsulation method in an ATM based network, and it can reduce overhead slightly compared to PPPoE.
PPPoE Passthrough	In addition to the ZyXEL Device's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the ZyXEL Device. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
ATM PVC Configuration - VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit)	
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
DSL Link Type	The DSL link type is set to **EoA** (Ethernet over ATM) to have an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. **EoA** supports IPoE, PPPoE and RFC1483/2684 bridging encapsulation methods.
Encapsulation Mode	The encapsulation method of multiplexing used by your is **LLC/SNAP-BRIDGING**. In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header.
Service Category	Select **UBR Without PCR** for applications that are non-time sensitive, such as e-mail. Select **CBR** (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustainable Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
PPP Information - This section is available only when you select **Routing** in the **Mode** field and **PPPoE** in the **WAN Service Type** field.	

Table 11 Broadband Add/Edit: Routing- PPPoE (continued)

Label	DESCRIPTION
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
PPP Password	Enter the password associated with the user name above.
PPPoE Service Name	Type the name of your PPPoE service here.
Authentication Method	The ZyXEL Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **AUTO**: Your ZyXEL Device accepts either CHAP or PAP when requested by this remote node. **PAP**: Your ZyXEL Device accepts PAP only. **CHAP**: Your ZyXEL Device accepts CHAP only. **MSCHAP**: Your ZyXEL Device accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.
Use Static IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you do not have a dynamic IP address.
IP Address	Enter the static IP address provided by your ISP. You will only see this field if you select **Use Static IP Address.**
Dial on Demand	Select **Dial on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Inactivity Timeout** field.
Inactivity Timeout	Specify an idle time-out in the **Inactivity Timeout** field when you select **Dial on Demand**.
MTU	The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field. For PPPoE, the MTU value is 1492.
Routing Feature	
NAT Enable	Select this option to activate NAT on this connection.
IGMP Proxy Enable	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Select this option to have the ZyXEL Device act as an IGMP proxy on this connection. This allows the ZyXEL Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the ZyXEL Device use the WAN interface of this connection as the system default gateway.
DNS Server - This section is not available when you select **Bridge** in the **WAN Service Type** field.	
Obtain DNS info Automatically	Select this to have the ZyXEL Device get the DNS server addresses from the ISP automatically.
Use the following Static DNS IP Address	Select this to have the ZyXEL Device use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.

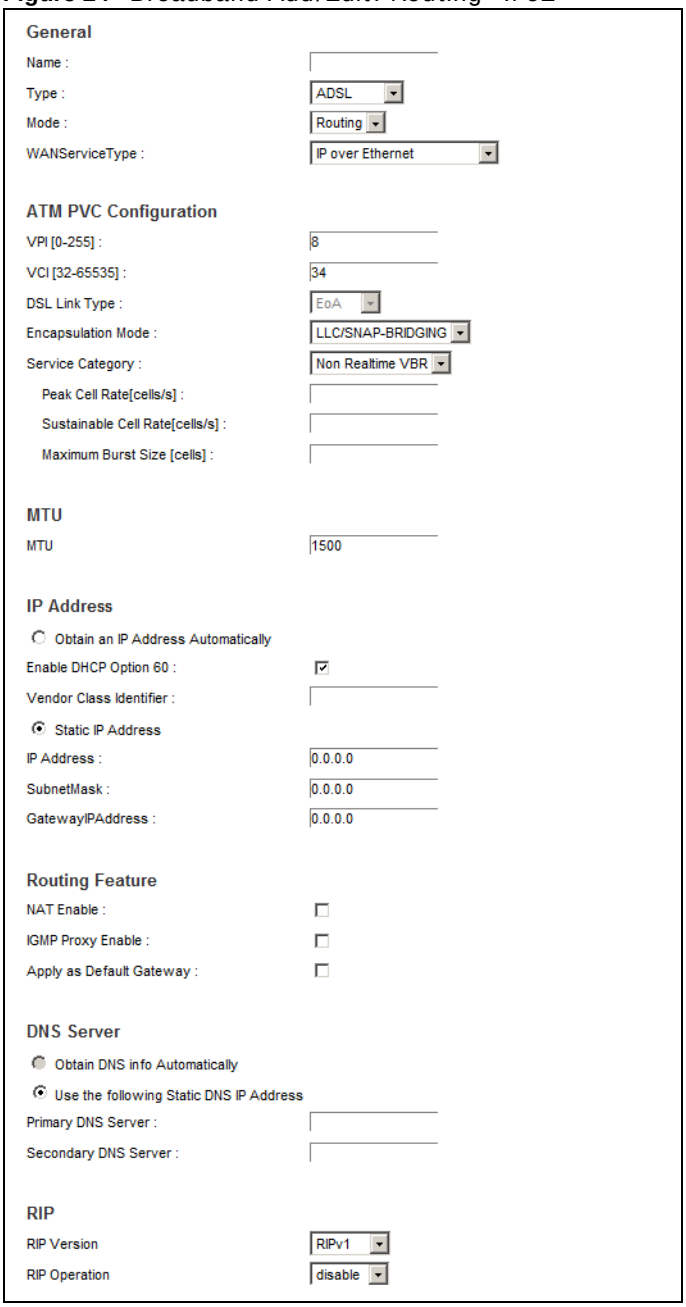
Table 11 Broadband Add/Edit: Routing- PPPoE (continued)

Label	DESCRIPTION
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

5.2.1.2 Routing- IPoE

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **Routing** as the encapsulation mode and **IPoE** as the WAN service type.

Figure 24 Broadband Add/Edit: Routing- IPoE



The following table describes the fields in this screen.

Table 12 Broadband Add/Edit: Routing- IPoE

Label	DESCRIPTION
General	
Name	Enter a service name of the connection.
Type	**ADSL**: The ZyXEL Device uses the ADSL technology for data transmission over the DSL port.
Mode	Select **Routing** (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account.
WAN Service Type	This field is available only when you select **Routing** in the **Mode** field. Select the method of encapsulation used by your ISP. • **PPP over Ethernet (PPPoE)** - PPPoE (Point to Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. Select this if you have a username and password for Internet access. • **IP over Ethernet** - In this type of Internet connection, IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. • **PPP over ATM** - PPPoA offers standard PPP features, such as authentication, encryption, and compression. It is used as the connection encapsulation method in an ATM based network, and it can reduce overhead slightly compared to PPPoE.
ATM PVC Configuration	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. This section is available only when you select **ADSL** in the **Type** field to configure an ATM layer-2 interface.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
DSL Link Type	The DSL link type is set to **EoA** (Ethernet over ATM) to have an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. **EoA** supports IPoE, PPPoE and RFC1483/2684 bridging encapsulation methods.
Encapsulation Mode	The encapsulation method of multiplexing used by your is **LLC/SNAP-BRIDGING**. In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header.
Service Category	Select **UBR Without PCR** for applications that are non-time sensitive, such as e-mail. Select **CBR** (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustainable Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.

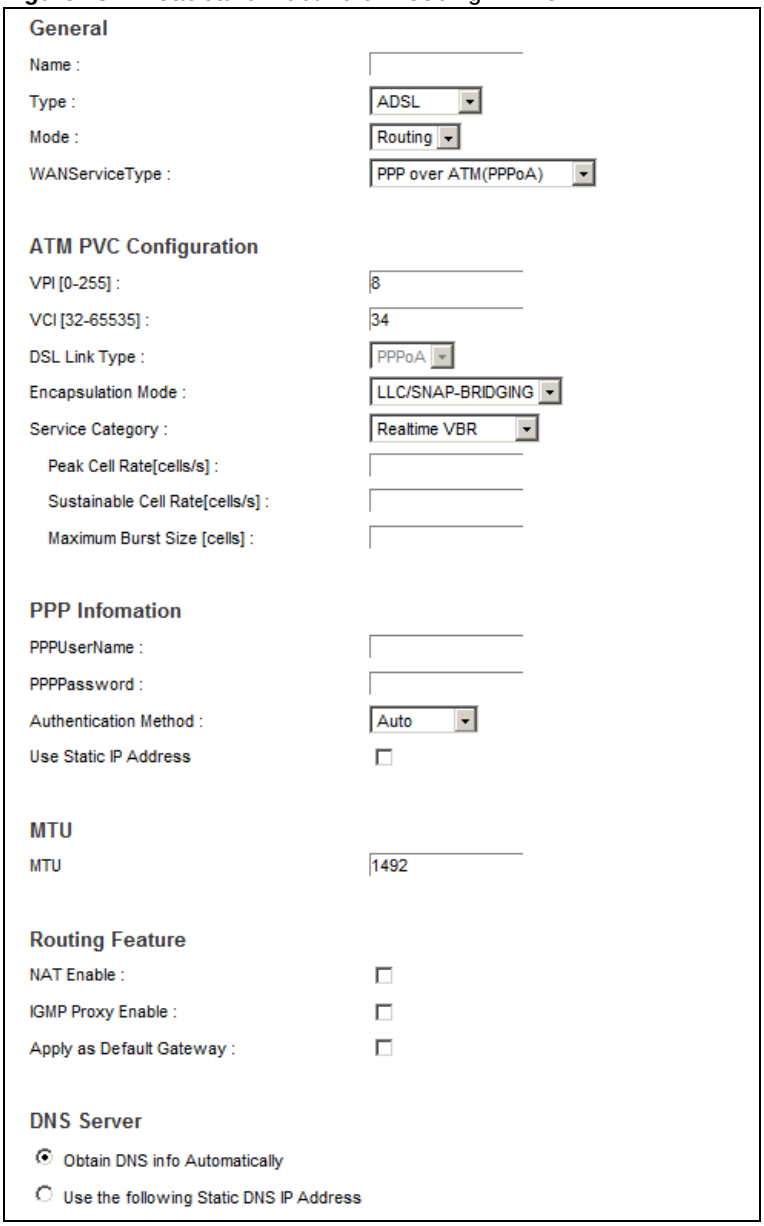
Table 12 Broadband Add/Edit: Routing- IPoE (continued)

Label	DESCRIPTION
MTU	The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field. For IPoE, the MTU value is 1500.
IP Address	This section is available only when you select **Routing** in the **Mode** field and **IPoE** in the **WAN Service Type** field.
Obtain an IP Address Automatically	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you have a dynamic IP address.
Enable DHCP Option 60	Select this to identify the vendor and functionality of the ZyXEL Device in DHCP requests that the ZyXEL Device sends to a DHCP server when getting a WAN IP address.
Vendor Class Identifier	Enter the Vendor Class Identifier (Option 60), such as the type of the hardware or firmware.
Static IP Address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter the static IP address provided by your ISP.
Subnet Mask	Enter the subnet mask provided by your ISP.
Gateway IP Address	Enter the gateway IP address provided by your ISP.
Routing Feature	
NAT Enable	Select this option to activate NAT on this connection.
IGMP Proxy Enable	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Select this option to have the ZyXEL Device act as an IGMP proxy on this connection. This allows the ZyXEL Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the ZyXEL Device use the WAN interface of this connection as the system default gateway.
DNS Server	This is available only when you select **Apply as Default Gateway** in the **Routing Feature** field.
Obtain DNS info Automatically	Select this to have the ZyXEL Device get the DNS server addresses from the ISP automatically.
Use the following Static DNS IP Address	Select this to have the ZyXEL Device use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
RIP	
RIP Version	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. This field is not configurable if you select disable in the **RIP Operation** field. Select the RIP version from **RIPv1**, **RIPv2** and **RIPv1v2**.
RIP Operation	Use this field to control how much routing information the ZyXEL Device sends and receives on the subnet. Select the RIP operation from **disable**, **passive** and **enable**.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

5.2.1.3 Routing- PPPoA

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **Routing** as the encapsulation mode and **PPPoA** as the WAN service type.

Figure 25 Broadband Add/Edit: Routing- PPPoA



The following table describes the fields in this screen.

Table 13 Broadband Add/Edit: Routing- PPPoA

Label	DESCRIPTION
General	
Name	Enter a service name of the connection.

Table 13 Broadband Add/Edit: Routing- PPPoA

Label	DESCRIPTION
Type	**ADSL**: The ZyXEL Device uses the ADSL technology for data transmission over the DSL port.
Mode	Select **Routing** (default) from the drop-down list box if your ISP give you one IP address only and you want multiple computers to share an Internet account.
WAN Service Type	This field is available only when you select **Routing** in the **Mode** field. Select the method of encapsulation used by your ISP. • **PPP over Ethernet (PPPoE)** - PPPoE (Point to Point Protocol over Ethernet) provides access control and billing functionality in a manner similar to dial-up services using PPP. Select this if you have a username and password for Internet access. • **IP over Ethernet** - In this type of Internet connection, IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. • **PPP over ATM** - PPPoA offers standard PPP features, such as authentication, encryption, and compression. It is used as the connection encapsulation method in an ATM based network, and it can reduce overhead slightly compared to PPPoE.
ATM PVC Configuration	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. This section is available only when you select **ADSL** in the **Type** field to configure an ATM layer-2 interface.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
DSL Link Type	The DSL link type is set to **EoA** (Ethernet over ATM) to have an Ethernet header in the packet, so that you can have multiple services/connections over one PVC. You can set each connection to have its own MAC address or all connections share one MAC address but use different VLAN IDs for different services. **EoA** supports IPoE, PPPoE and RFC1483/2684 bridging encapsulation methods.
Encapsulation Mode	The encapsulation method of multiplexing used by your is **LLC/SNAP-BRIDGING**. In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header.
Service Category	Select **UBR Without PCR** for applications that are non-time sensitive, such as e-mail. Select **CBR** (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustainable Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
IP Address	This section is available only when you select **Routing** in the **Mode** field and **IPoE** in the **WAN Service Type** field.
PPP Information - This section is available only when you select **Routing** in the **Mode** field and **PPPoE** in the **WAN Service Type** field.	
PPP User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.

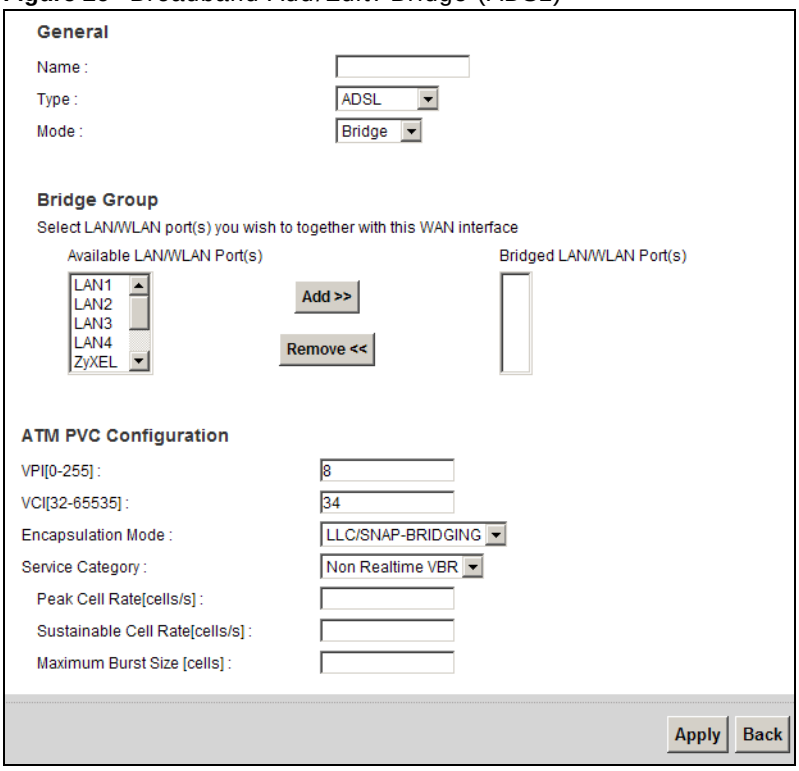
Table 13 Broadband Add/Edit: Routing- PPPoA

Label	DESCRIPTION
PPP Password	Enter the password associated with the user name above.
Authentication Method	The ZyXEL Device supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **AUTO**: Your ZyXEL Device accepts either CHAP or PAP when requested by this remote node. **PAP**: Your ZyXEL Device accepts PAP only. **CHAP**: Your ZyXEL Device accepts CHAP only. **MSCHAP**: Your ZyXEL Device accepts MSCHAP only. MS-CHAP is the Microsoft version of the CHAP.
Use Static IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select this if you do not have a dynamic IP address.
IP Address	Enter the static IP address provided by your ISP. You will only see this field if you select **Use Static IP Address**
MTU	The Maximum Transmission Unit (MTU) defines the size of the largest packet allowed on an interface or connection. Enter the MTU in this field. For PPPoA and the default MTU is 1492.
Routing Feature	
NAT Enable	Select this option to activate NAT on this connection.
IGMP Proxy Enable	Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. Select this option to have the ZyXEL Device act as an IGMP proxy on this connection. This allows the ZyXEL Device to get subscribing information and maintain a joined member list for each multicast group. It can reduce multicast traffic significantly.
Apply as Default Gateway	Select this option to have the ZyXEL Device use the WAN interface of this connection as the system default gateway.
DNS Server - This section is not available when you select **Bridge** in the **WAN Service Type** field.	
Obtain DNS info Automatically	Select this to have the ZyXEL Device get the DNS server addresses from the ISP automatically.
Use the following Static DNS IP Address	Select this to have the ZyXEL Device use the DNS server addresses you configure manually.
Primary DNS Server	Enter the first DNS server address assigned by the ISP.
Secondary DNS Server	Enter the second DNS server address assigned by the ISP.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

5.2.1.4 Bridge Mode

Click the **Add new WAN Interface** in the **Network Setting > Broadband** screen or the **Edit** icon next to the connection you want to configure. Select **Bridge** as the encapsulation mode. The following screen appears.

Figure 26 Broadband Add/Edit: Bridge (ADSL)



The following table describes the fields in this screen.

Table 14 Broadband Add/Edit: Bridge (ADSL)

Label	DESCRIPTION
General	
Name	Enter a service name of the connection.
Type	Select **ADSL** as the interface for which you want to configure here. The ZyXEL Device uses the ADSL technology for data transmission over the DSL port.
Mode	Select **Bridge** when your ISP provides you more than one IP address and you want the connected computers to get individual IP address from ISP's DHCP server directly. If you select **Bridge**, you cannot use routing functions, such as QoS, Firewall, DHCP server and NAT on traffic from the selected LAN port(s).
Bridge Group	Select the LAN/WLAN port(s) from which traffic will be forwarded to the WAN interface directly. Select a port from the **Available LAN / WLAN Port(s)** list and click **Add > >** to add it to the **Bridged LAN / WLAN Port(s)** list. If you want to remove a port from the **Bridged LAN / WLAN Port(s)** list, select it and click **Remove < <**. You cannot configure a QoS class for traffic from the LAN port which is selected here.
ATM PVC Configuration	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. This section is available only when you select **ADSL** in the **Type** field to configure an ATM layer-2 interface.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.

Table 14 Broadband Add/Edit: Bridge (ADSL) (continued)

Label	DESCRIPTION
Encapsulation Mode	The encapsulation method of multiplexing used by your is **LLC/SNAP-BRIDGING**. In LCC encapsulation, bridged PDUs are encapsulated by identifying the type of the bridged media in the SNAP header.
Service Category	Select **UBR Without PCR** for applications that are non-time sensitive, such as e-mail. Select **CBR** (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **Non Realtime VBR** (non real-time Variable Bit Rate) for connections that do not require closely controlled delay and delay variation. Select **Realtime VBR** (real-time Variable Bit Rate) for applications with bursty connections that require closely controlled delay and delay variation.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustainable Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

5.3 Technical Reference

The following section contains additional technical information about the ZyXEL Device features described in this chapter.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The ZyXEL Device can work in bridge mode or routing mode. When the ZyXEL Device is in routing mode, it supports the following methods.

IP over Ethernet

IP over Ethernet (IPoE) is an alternative to PPPoE. IP packets are being delivered across an Ethernet network, without using PPP encapsulation. They are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged Ethernet cells.

PPP over Ethernet

Point-to-Point Protocol over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the ZyXEL Device (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the ZyXEL Device does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

PPP over ATM

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The ZyXEL Device encapsulates the PPP session based on RFC 1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to RFC 1483 for more detailed information.

Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

Traffic Shaping

Traffic Shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate

congestion, which is important for transmission of real time data such as audio and video connections.

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

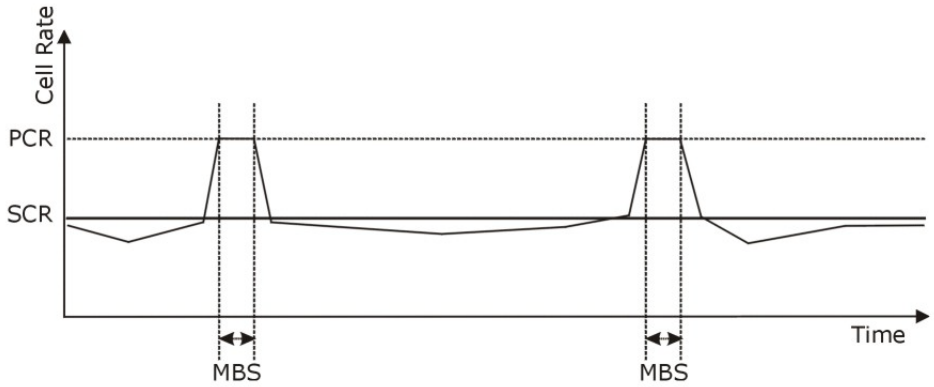
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 27 Example of Traffic Shaping



ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

Constant Bit Rate (CBR)

Constant Bit Rate (CBR) provides fixed bandwidth that is always available even if no data is being sent. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. A PCR is specified and if traffic exceeds this rate, cells may be dropped. Examples of connections that need CBR would be high-resolution video and voice.

Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (VBR-RT) or non-real time (VBR-nRT) connections.

The VBR-RT (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. It also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example of an VBR-RT connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The VBR-nRT (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. It is commonly used for "bursty" traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example of an VBR-nRT connection would be non-time sensitive data file transfers.

Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is for bursty data transfers. However, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. An example application is background file transfer.

IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and default gateway.

Introduction to VLANs

A Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In Multi-Tenant Unit (MTU) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Multicast

IP packets are transmitted in either one of two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

Internet Group Multicast Protocol (IGMP) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group

and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

At start up, the ZyXEL Device queries all directly connected networks to gather group membership. After that, the ZyXEL Device periodically updates this information.

DNS Server Address Assignment

Use Domain Name System (DNS) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The ZyXEL Device can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, manually enter them in the DNS server fields.

2 If your ISP dynamically assigns the DNS server IP addresses (along with the ZyXEL Device's WAN IP address), set the DNS server fields to get the DNS server address from the ISP.

6

Wireless

6.1 Overview

This chapter describes the ZyXEL Device's **Network Setting > Wireless** screens. Use these screens to set up your ZyXEL Device's wireless connection.

6.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable the Wireless LAN, enter the SSID and select the wireless security mode (Section 6.2 on page 107).
- Use the **More AP** screen to set up multiple wireless networks on your ZyXEL Device (Section 6.3 on page 113).
- Use the **WPS** screen to enable or disable WPS, view or generate a security PIN (Personal Identification Number) (Section 6.4 on page 115).
- Use the **WMM** screen to enable Wi-Fi MultiMedia (WMM) to ensure quality of service in wireless networks for multimedia applications (Section 6.5 on page 117).
- Use the **Scheduling** screen to schedule a time period for the wireless LAN to operate each day (Section 6.6 on page 118).

You don't necessarily need to use all these screens to set up your wireless connection. For example, you may just want to set up a network name, a wireless radio channel and some security in the **General** screen.

6.1.2 Wireless Network Overview

Wireless networks consist of wireless clients, access points and bridges.

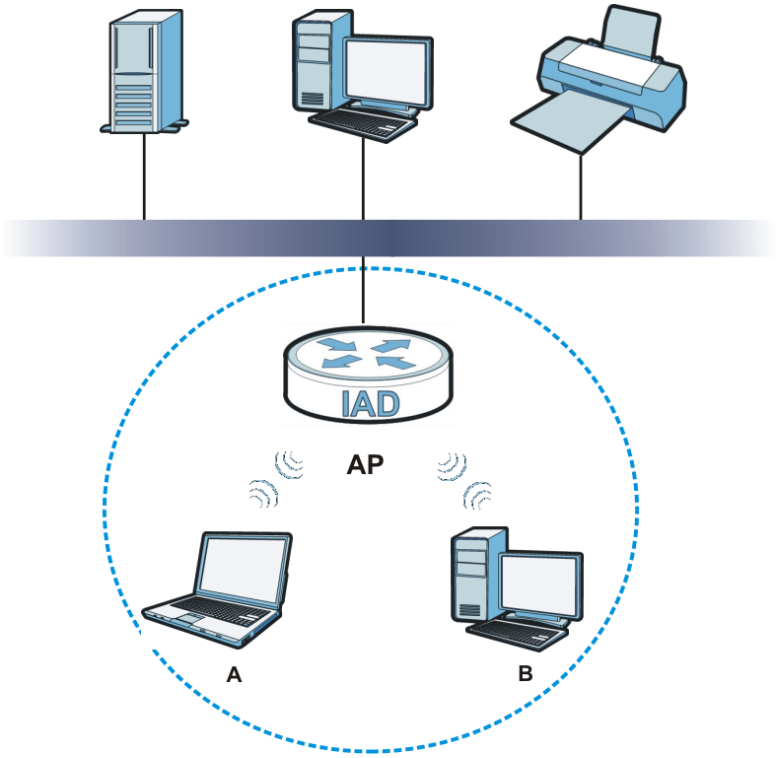
- A wireless client is a radio connected to a user's computer.
- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

The following figure provides an example of a wireless network.

Figure 28 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your ZyXEL Device is the AP.

Every wireless network must follow these basic guidelines:

- Every device in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentifier.
- If two wireless networks overlap, they should use a different channel.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every device in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

6.1.3 Before You Begin

Before you start using these screens, ask yourself the following questions. See Section 6.7 on page 119 if some of the terms used here do not make sense to you.

- What wireless standards do the other wireless devices support (IEEE 802.11g, for example)? What is the most appropriate standard to use?
- What security options do the other wireless devices support (WPA-PSK, for example)? What is the best one to use?
- Do the other wireless devices support WPS (Wi-Fi Protected Setup)? If so, you can set up a well-secured network very easily.

  Even if some of your devices support WPS and some do not, you can use WPS to set up your network and then add the non-WPS devices manually, although this is somewhat more complicated to do.
- What advanced options do you want to configure, if any? If you want to configure advanced options, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them alone.

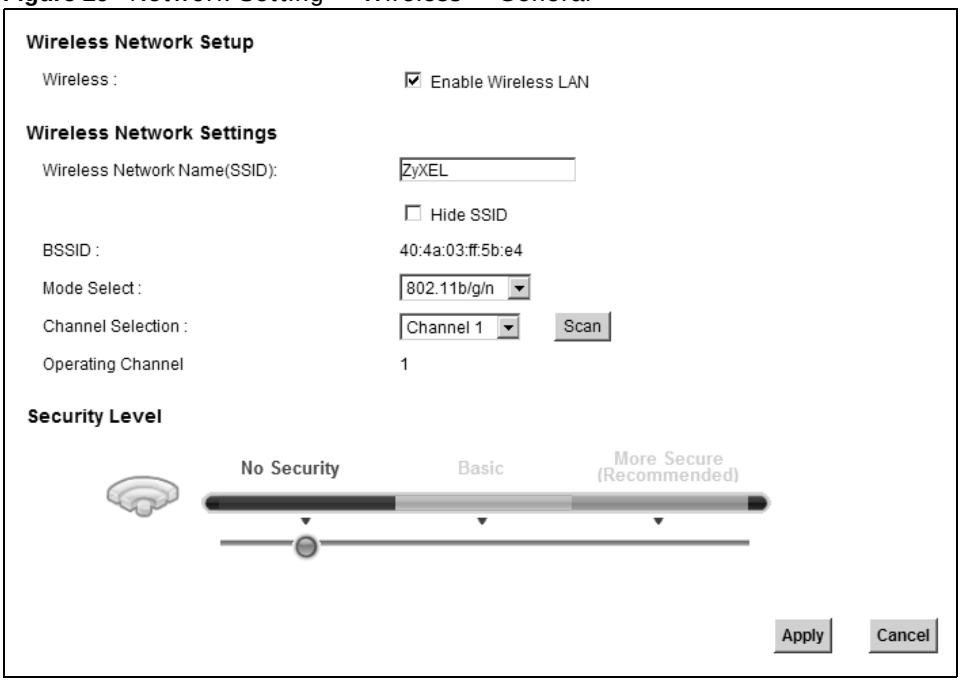
6.2 The Wireless General Screen

Use this screen to enable the Wireless LAN, enter the SSID and select the wireless security mode.

Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.

Click **Network Setting > Wireless** to open the **General** screen.

Figure 29 Network Setting > Wireless > General



The following table describes the labels in this screen.

Table 15 Network > Wireless LAN > General

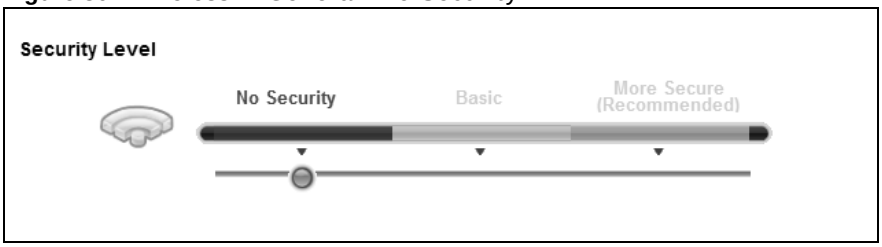
LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Select the **Enable Wireless LAN** check box to activate the wireless LAN.
Wireless Network Settings	
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
BSSID	This shows the MAC address of the wireless interface on the ZyXEL Device when wireless LAN is enabled.
Mode Select	This makes sure that only compliant WLAN devices can associate with the ZyXEL Device. Select **802.11b/g/n** to allow IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced. Select **802.11b/g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select **802.11n only in 2.4G band** to allow only IEEE 802.11n compliant WLAN devices with the same frequency range (2.4 GHz) to associate with the ZyXEL Device.
Channel Selection	Set the channel depending on your particular region. Select a channel or use **Auto** to have the ZyXEL Device automatically determine a channel to use. If you are having problems with wireless interference, changing the channel may help. Try to use a channel that is as many channels away from any channels used by neighboring APs as possible. The channel number which the ZyXEL Device is currently using then displays in the **Operating Channel** field.
Scan	Click this button to have the ZyXEL Device immediately scan for and select a channel (which is not used by another device) whenever the device reboots or the wireless setting is changed.
Operating Channel	This is the channel currently being used by your AP.
Security Level	
Security Mode	Select **Basic** or **More Secure** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the ZyXEL Device. When you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See the following sections for more details about wireless security modes.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Cancel	Click **Cancel** to restore your previously saved settings.

6.2.1 No Security

Select **No Security** to allow wireless stations to communicate with the access points without any data encryption or authentication.

Note: If you do not enable any wireless security on your ZyXEL Device, your network is accessible to any wireless networking device that is within range.

Figure 30 Wireless > General: No Security



The following table describes the labels in this screen.

Table 16 Wireless > General: No Security

LABEL	DESCRIPTION
Security Level	Choose **No Security** from the sliding bar.

6.2.2 Basic (Static WEP/Shared WEP Encryption)

WEP encryption scrambles the data transmitted between the wireless stations and the access points (AP) to keep network communications private. Both the wireless stations and the access points must use the same WEP key.

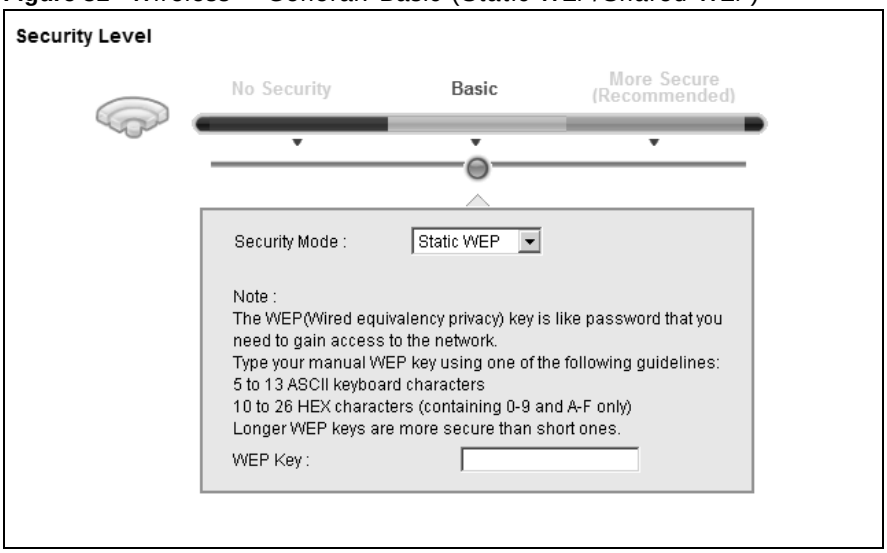
There are two types of WEP authentication namely, Open System (**Static WEP**) and Shared Key (**Shared WEP**).

Open system is implemented for ease-of-use and when security is not an issue. The wireless station and the AP or peer computer do not share a secret key. Thus the wireless stations can associate with any AP or peer computer and listen to any transmitted data that is not encrypted.

Shared key mode involves a shared secret key to authenticate the wireless station to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless station and the AP or peer computer.

In order to configure and enable WEP encryption, click **Network Settings > Wireless** to display the **General** screen. Select **Basic** as the security level. Then select **Static WEP** or **Shared WEP** from the **Security Mode** list.

Figure 31 Wireless > General: Basic (Static WEP/Shared WEP)


Security Level
No Security
Basic
More Secure
(Recommended)
Security Mode :
Static WEP
Note :
The WEP(Wired equivalency privacy) key is like password that you need to gain access to the network.
Type your manual WEP key using one of the following guidelines:
5 to 13 ASCII keyboard characters
10 to 26 HEX characters (containing 0-9 and A-F only)
Longer WEP keys are more secure than short ones.
WEP Key :

The following table describes the labels in this screen.

Table 17 Wireless > General: Basic (Static WEP/Shared WEP)

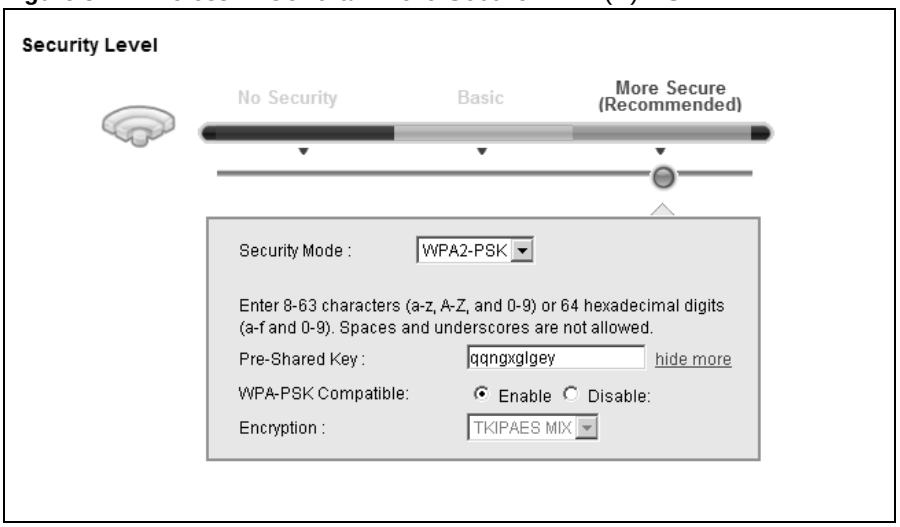
LABEL	DESCRIPTION
Security Mode	Choose **Static WEP** or **Shared WEP** from the drop-down list box. • Select **Static WEP** to have the ZyXEL Device allow association with wireless clients that use Open System mode. Data transfer is encrypted as long as the wireless client has the correct WEP key for encryption. The ZyXEL Device authenticates wireless clients using Shared Key mode that have the correct WEP key. • Select **Shared WEP** to have the ZyXEL Device authenticate only those wireless clients that use Shared Key mode and have the correct WEP key.
WEP Key	Enter a WEP key that will be used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. If you want to manually set the WEP key, enter any 5 or 13 characters (ASCII string) or 10 or 26 hexadecimal characters ("0-9", "A-F") for a 64-bit or 128-bit WEP key respectively.

6.2.3 More Secure (WPA(2)-PSK)

The WPA-PSK security mode provides both improved data encryption and user authentication over WEP. Using a Pre-Shared Key (PSK), both the ZyXEL Device and the connecting client share a common password in order to validate the connection. This type of encryption, while robust, is not as strong as WPA, WPA2 or even WPA2-PSK. The WPA2-PSK security mode is a newer, more robust version of the WPA encryption standard. It offers slightly better security, although the use of PSK makes it less robust than it could be.

Click **Network Settings** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA-PSK** or **WPA2-PSK** from the **Security Mode** list.

Figure 32 Wireless > General: More Secure: WPA(2)-PSK



The following table describes the labels in this screen.

Table 18 Wireless > General: WPA(2)-PSK

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA(2)-PSK data encryption.
Security Mode	Select **WPA-PSK** or **WPA2-PSK** from the drop-down list box.
Pre-Shared Key	The encryption mechanisms used for **WPA / WPA2** and **WPA-PSK / WPA2-PSK** are the same. The only difference between the two is that **WPA-PSK / WPA2-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters or 64 hexidecimal digits.
more.../hide more	Click **more...** to show more fields in this section. Click **hide more** to hide them.

Table 18 Wireless > General: WPA(2)-PSK (continued)

LABEL	DESCRIPTION
WPA-PSK Compatible	This field appears when you choose **WPA-PSK2** as the **Security Mode**. Check this field to allow wireless devices using **WPA-PSK** security mode to connect to your ZyXEL Device. The ZyXEL Device supports WPA-PSK and WPA2-PSK simultaneously.
Encryption	If the security mode is **WPA-PSK**, the encryption mode is set to **TKIP** to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network. If the security mode is **WPA-PSK2** and **WPA-PSK Compatible** is disabled, the encryption mode is set to **AES** to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP. If the security mode is **WPA-PSK2** and **WPA-PSK Compatible** is enabled, the encryption mode is set to **TKIPAES MIX** to allow both TKIP and AES types of security in your wireless network.

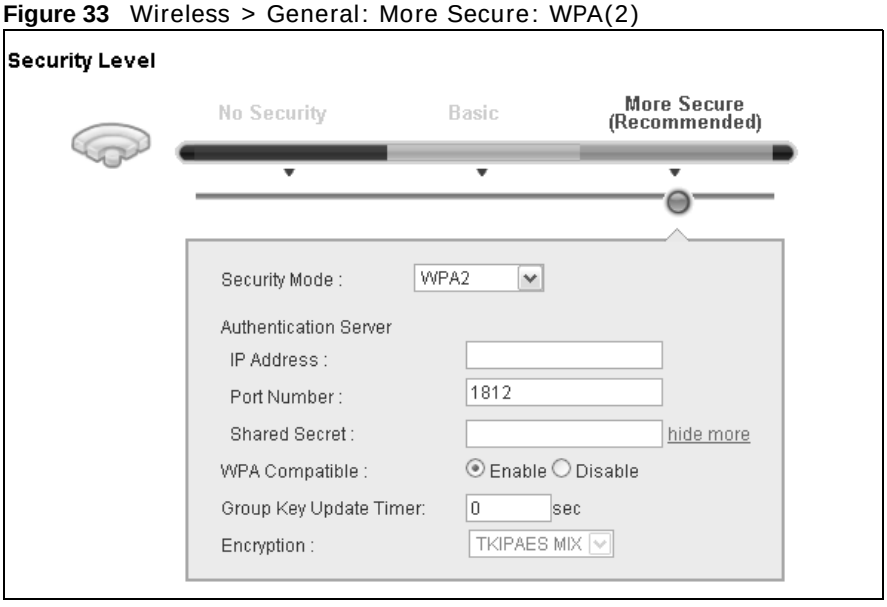
6.2.4 WPA(2) Authentication

The WPA2 security mode is currently the most robust form of encryption for wireless networks. It requires a RADIUS server to authenticate user credentials and is a full implementation the security protocol. Use this security option for maximum protection of your network. However, it is the least backwards compatible with older devices.

The WPA security mode is a security subset of WPA2. It requires the presence of a RADIUS server on your network in order to validate user credentials. This encryption standard is slightly older than WPA2 and therefore is more compatible with older devices.

Click **Network Settings** > **Wireless** to display the **General** screen. Select **More Secure** as the security level. Then select **WPA** or **WPA2** from the **Security Mode** list.

Figure 33 Wireless > General: More Secure: WPA(2)



The following table describes the labels in this screen.

Table 19 Wireless > General: More Secure: WPA(2)

LABEL	DESCRIPTION
Security Level	Select **More Secure** to enable WPA(2)-PSK data encryption.
Security Mode	Choose **WPA** or **WPA2** from the drop-down list box.
Authentication Server	
IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	Enter the port number of the external authentication server. The default port number is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network.
more.../hide more	Click **more...** to show more fields in this section. Click **hide more** to hide them.
WPA Compatible	This field is only available for WPA2. Select this if you want the ZyXEL Device to support WPA and WPA2 simultaneously.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the RADIUS server sends a new group key out to all clients.
Encryption	If the security mode is **WPA**, the encryption mode is set to **TKIP** to enable Temporal Key Integrity Protocol (TKIP) security on your wireless network. If the security mode is **WPA2**, the encryption mode is set to **AES** to enable Advanced Encryption System (AES) security on your wireless network. AES provides superior security to TKIP.

6.3 The More AP Screen

The ZyXEL Device can broadcast up to four wireless network names at the same time. This means that users can connect to the ZyXEL Device using different SSIDs. You can secure the connection on each SSID profile so that wireless clients connecting to the ZyXEL Device using different SSIDs cannot communicate with each other.

This screen allows you to enable and configure multiple Basic Service Sets (BSSs) on the ZyXEL Device.

Click **Network Settings > Wireless** > **More AP**. The following screen displays.

Figure 34 Network Settings > Wireless > More AP

#	Active	SSID	Security	Modify
2		ZyXEL2	WPA2-PSK	
3		ZyXEL3	WPA2-PSK	
4		ZyXEL4	WPA2-PSK	

The following table describes the labels in this screen.

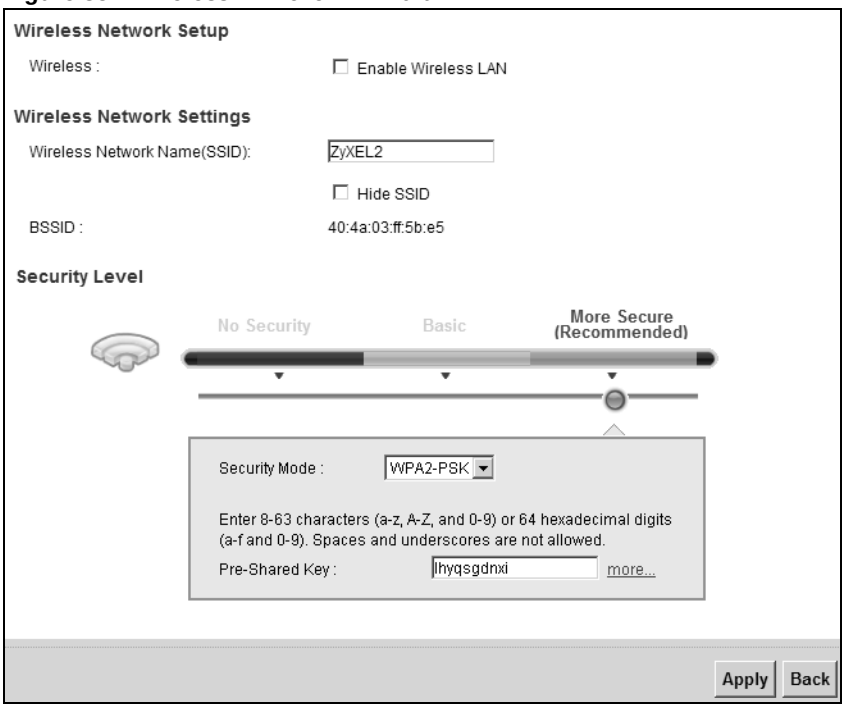
Table 20 Network Settings > Wireless > More AP

LABEL	DESCRIPTION
#	This is the index number of the entry.
Active	This field indicates whether this SSID is active. A yellow bulb signifies that this SSID is active. A gray bulb signifies that this SSID is not active.
SSID	An SSID profile is the set of parameters relating to one of the ZyXEL Device's BSSs. The SSID (Service Set IDentifier) identifies the Service Set with which a wireless device is associated. This field displays the name of the wireless profile on the network. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Security	This field indicates the security mode of the SSID profile.
Modify	Click the **Edit** icon to configure the SSID profile.

6.3.1 Edit More AP

Use this screen to edit an SSID profile. Click the **Edit** icon next to an SSID in the **More AP** screen. The following screen displays.

Figure 35 Wireless > More AP: Edit



The following table describes the fields in this screen.

Table 21 Wireless > More AP: Edit

LABEL	DESCRIPTION
Wireless Network Setup	
Wireless	Select the **Enable Wireless LAN** check box to activate the wireless LAN.
Wireless Network Settings	

Table 21 Wireless > More AP: Edit

LABEL	DESCRIPTION
Wireless Network Name (SSID)	The SSID (Service Set IDentity) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same SSID. Enter a descriptive name (up to 32 English keyboard characters) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
BSSID	This shows the MAC address of the wireless interface on the ZyXEL Device when wireless LAN is enabled.
Security Level	
Security Mode	Select **Basic (WEP)** or **More Secure (WPA(2)-PSK, WPA(2))** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as the ZyXEL Device. After you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without any data encryption or authentication. See Section 6.2.1 on page 109 for more details about this field.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

6.4 The WPS Screen

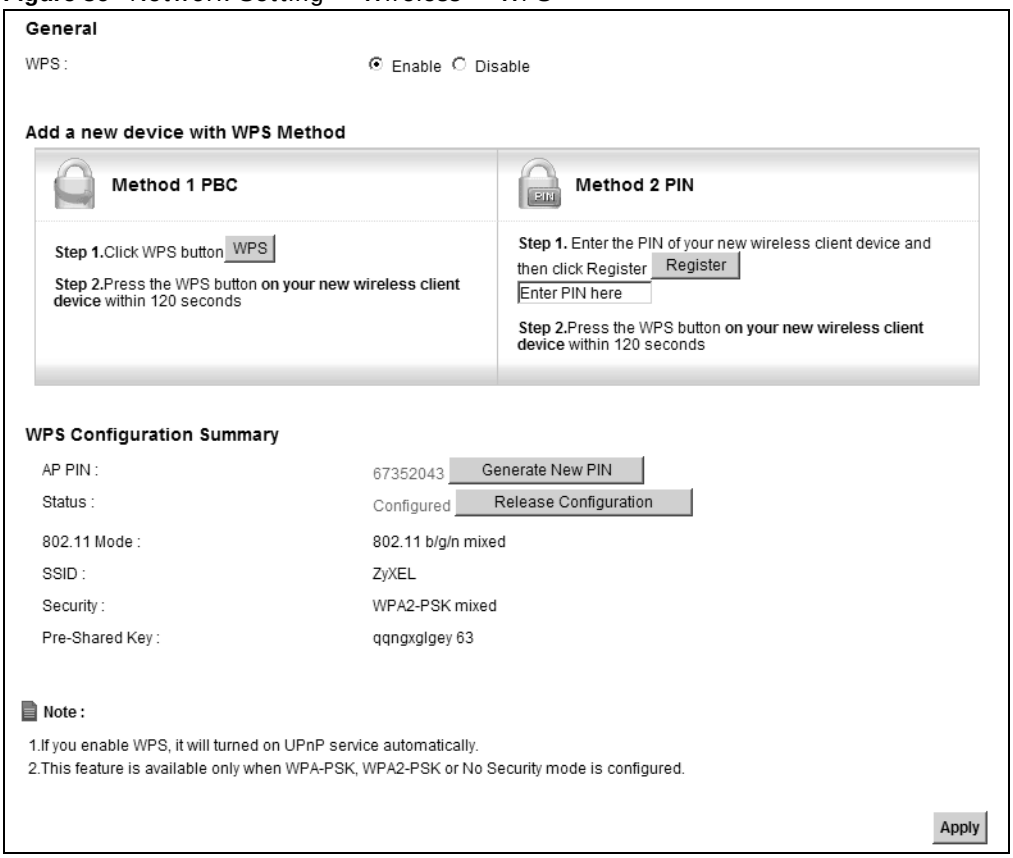
Use this screen to configure WiFi Protected Setup (WPS) on your ZyXEL Device.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Set up each WPS connection between two devices. Both devices must support WPS. See Section 6.7.6.3 on page 125 for more information about WPS.

Note: The ZyXEL Device applies the security settings of the **SSID1** profile (see Section 6.2 on page 107). If you want to use the WPS feature, make sure you have set the security mode of **SSID1** to **WPA-PSK**, **WPA2-PSK** or **No Security**.

Click **Network Setting > Wireless > WPS**. The following screen displays. Select **Enable** and click **Apply** to activate the WPS function. Then you can configure the WPS settings in this screen.

Figure 36 Network Setting > Wireless > WPS


General
WPS :
Enable
Disable
Add a new device with WPS Method
Method 1 PBC
Step 1.Click WPS button
WPS
Step 2.Press the WPS button on your new wireless client device within 120 seconds
Method 2 PIN
Step 1. Enter the PIN of your new wireless client device and then click Register
Register
Enter PIN here
Step 2.Press the WPS button on your new wireless client device within 120 seconds
WPS Configuration Summary
AP PIN :
67352043
Generate New PIN
Status :
Configured
Release Configuration
802.11 Mode :
802.11 b/g/n mixed
SSID :
ZyXEL
Security :
WPA2-PSK mixed
Pre-Shared Key :
qqngxglgey 63
Note :
1.If you enable WPS, it will turned on UPnP service automatically.
2.This feature is available only when WPA-PSK, WPA2-PSK or No Security mode is configured.
Apply

The following table describes the labels in this screen.

Table 22 Network Setting > Wireless > WPS

LABEL	DESCRIPTION
Enable WPS	Select **Enable** to activate WPS on the ZyXEL Device.
Add a new device with WPS Method	
Method 1 PBC	Use this section to set up a WPS wireless network using Push Button Configuration (PBC).
WPS	Click this button to add another WPS-enabled wireless device (within wireless range of the ZyXEL Device) to your wireless network. This button may either be a physical button on the outside of device, or a menu button similar to the **WPS** button on this screen. Note: You must press the other wireless device's WPS button within two minutes of pressing this button.
Method 2 PIN	Use this section to set up a WPS wireless network by entering the PIN (Personal Identification Number) of the client into the ZyXEL Device.
Register	Enter the PIN of the device that you are setting up a WPS connection with and click **Register** to authenticate and add the wireless device to your wireless network. You can find the PIN either on the outside of the device, or by checking the device's settings. Note: You must also activate WPS on that device within two minutes to have it present its PIN to the ZyXEL Device.
WPS Configuration Summary	

Table 22 Network Setting > Wireless > WPS (continued)

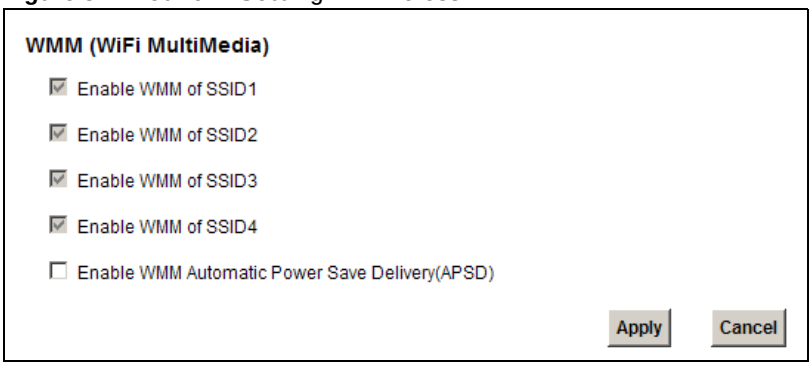
LABEL	DESCRIPTION
AP PIN	The PIN of the ZyXEL Device is shown here. Enter this PIN in the configuration utility of the device you want to connect to using WPS. The PIN is not necessary when you use WPS push-button method. Click the **Generate New PIN** button to have the ZyXEL Device create a new PIN.
Status	This field displays **Configured** when the ZyXEL Device has been configured, and a wireless client can connect to the ZyXEL Device through WPS. It displays **Unconfigured** if the ZyXEL Device has not been configured for WPS, and wireless clients will not be able to establish a link with the device through WPS. **Release Configuration** removes the configured wireless security settings in the ZyXEL Device.
Release Configuration	This button is available when the WPS status is **Configured.** Click this button to remove all configured wireless and wireless security settings for WPS connections on the ZyXEL Device.
802.11 Mode	This is the 802.11 mode used. Only compliant WLAN devices can associate with the ZyXEL Device.
SSID	This is the name of the wireless network.
Security	This is the type of wireless security employed by the network.
Apply	Click **Apply** to save your changes.

6.5 The WMM Screen

Use this screen to enable or disable Wi-Fi MultiMedia (WMM) wireless networks for multimedia applications.

Click **Network Setting > Wireless > WMM**. The following screen displays.

Figure 37 Network Setting > Wireless > WMM



The following table describes the labels in this screen.

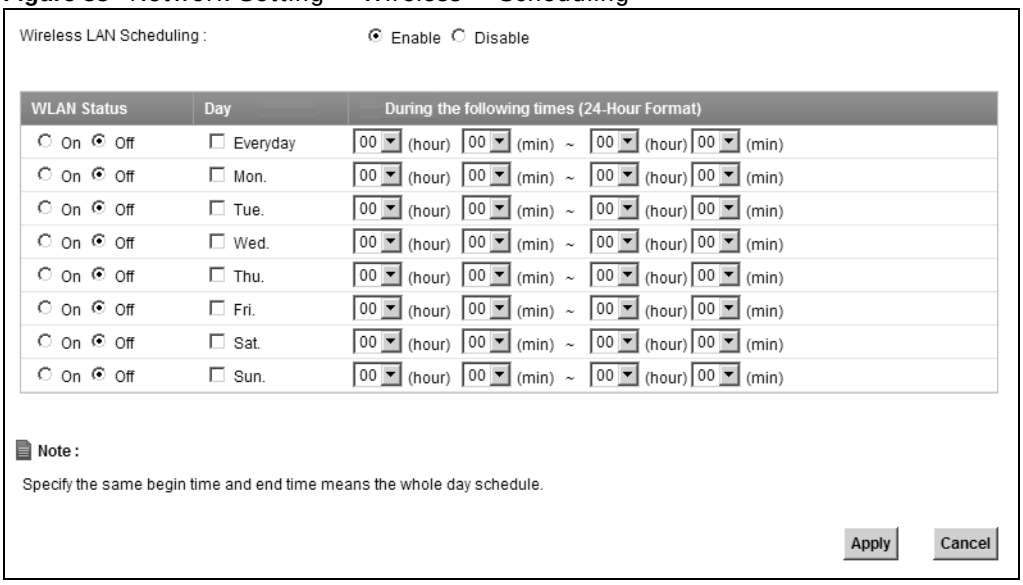
Table 23 Network Setting > Wireless > WMM

LABEL	DESCRIPTION
Enable WMM of SSID1~4	This enables the ZyXEL Device to automatically give a service a priority level according to the ToS value in the IP header of packets it sends. WMM QoS (Wifi MultiMedia Quality of Service) gives high priority to voice and video, which makes them run more smoothly.
Enable WMM Automatic Power Save Deliver (APSD)	Click this to increase battery life for battery-powered wireless clients. APSD uses a longer beacon interval when transmitting traffic that does not require a short packet exchange interval.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.6 Scheduling Screen

Click **Network Setting > Wireless > Scheduling** to open the **Wireless LAN Scheduling** screen. Use this screen to configure when the ZyXEL Device enables or disables the wireless LAN.

Figure 38 Network Setting > Wireless > Scheduling



The following table describes the labels in this screen.

Table 24 Network Setting > Wireless > Scheduling

LABEL	DESCRIPTION
Wireless LAN Scheduling	Select **Enable** to activate wireless LAN scheduling on your ZyXEL Device.
WLAN status	Select **On** or **Off** to enable or disable the wireless LAN.
Day	Select the day(s) you want to turn the wireless LAN on or off.
During the following times	Specify the time period during which to apply the schedule. For example, you want the wireless network to be only available during work hours. Check Mon ~ Fri in the day column, and specify 8:00 ~ 18:00 in the time table.

Table 24 Network Setting > Wireless > Scheduling

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

6.7 Technical Reference

This section discusses wireless LANs in depth. For more information, see the appendix.

6.7.1 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the ZyXEL Device's web configurator.

Table 25 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the ZyXEL Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the ZyXEL Device.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the ZyXEL Device does, it cannot communicate with the ZyXEL Device.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

6.7.2 Wireless Security Overview

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network, he or she can steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Protocol (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is very secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess - for example, a three-letter word from the dictionary.

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

The following sections introduce different types of wireless security you can set up in the wireless network.

6.7.2.1 SSID

Normally, the ZyXEL Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the ZyXEL Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

6.7.2.2 MAC Address Filter

Every device that can use a wireless network has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each device in the wireless network, see the device's User's Guide or other documentation.

You can use the MAC address filter to tell the ZyXEL Device which devices are allowed or not allowed to use the wireless network. If a device is allowed to use the wireless network, it still has to have the correct information (SSID, channel, and security). If a device is not allowed to use the wireless network, it does not matter if it has the correct information.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized wireless devices to get the MAC address of an authorized device. Then, they can use that MAC address to use the wireless network.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

6.7.2.3 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before using it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

6.7.2.4 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See Section 6.7.2.3 on page 121 for information about this.)

Table 26 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	WPA
↕	Static WEP	
	WPA-PSK	
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose **WPA** or **WPA2**. If users do not log in to the wireless network, you can choose no encryption, **Static WEP**, **WPA-PSK**, or **WPA2-PSK**.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the ZyXEL Device and you do not have a RADIUS server. Therefore, there is no authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **Static WEP** in the wireless network.

Note: It is recommended that wireless networks use **WPA-PSK**, **WPA**, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

When you select **WPA2** or **WPA2-PSK** in your ZyXEL Device, you can also select an option (**WPA compatible**) to support WPA as well. In this case, if some of the devices support WPA and some support WPA2, you should set up **WPA2-PSK** or **WPA2** (depending on the type of wireless network login) and select the **WPA compatible** option in the ZyXEL Device.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

6.7.3 Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

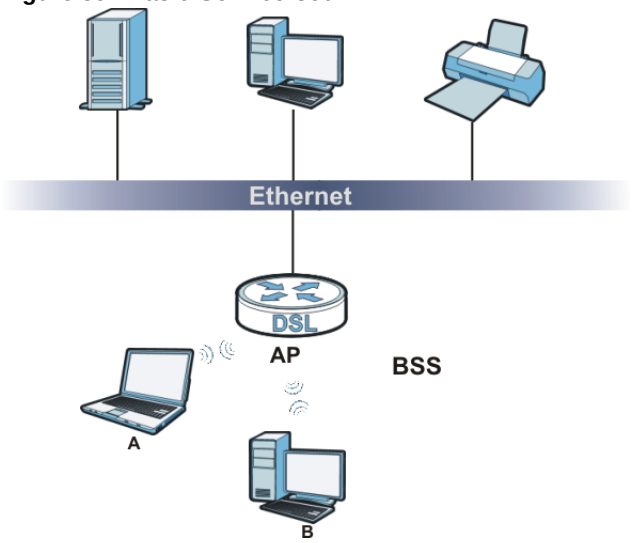
Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

6.7.4 BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS traffic blocking is disabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS traffic blocking is enabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 39 Basic Service set



6.7.5 MBSSID

Traditionally, you need to use different APs to configure different Basic Service Sets (BSSs). As well as the cost of buying extra APs, there is also the possibility of channel interference. The ZyXEL Device's MBSSID (Multiple Basic Service Set IDentifier) function allows you to use one access point to provide several BSSs simultaneously. You can then assign varying QoS priorities and/or security modes to different SSIDs.

Wireless devices can use different BSSIDs to associate with the same AP.

6.7.5.1 Notes on Multiple BSSs

- A maximum of eight BSSs are allowed on one AP simultaneously.
- You must use different keys for different BSSs. If two wireless devices have different BSSIDs (they are in different BSSs), but have the same keys, they may hear each other's communications (but not communicate with each other).
- MBSSID should not replace but rather be used in conjunction with 802.1x security.

6.7.6 WiFi Protected Setup (WPS)

Your ZyXEL Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

6.7.6.1 Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the ZyXEL Device, see Section 6.4 on page 115).
3. Press the button on one of the devices (it doesn't matter which). For the ZyXEL Device you must press the WPS button for more than three seconds.
4. Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

   If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

6.7.6.2 PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (in some devices you can generate a new PIN by clicking on a button in the configuration interface).

Use the PIN method instead of the push-button configuration (PBC) method if you want to ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in range of each other. However, you need to log into the configuration interfaces of both devices to use the PIN method.

When you use the PIN method, you must enter the PIN from one device (usually the wireless client) into the second device (usually the Access Point or wireless router). Then, when WPS is activated on the first device, it presents its PIN to the second device. If the PIN matches, one device sends the network and security information to the other, allowing it to join the network.

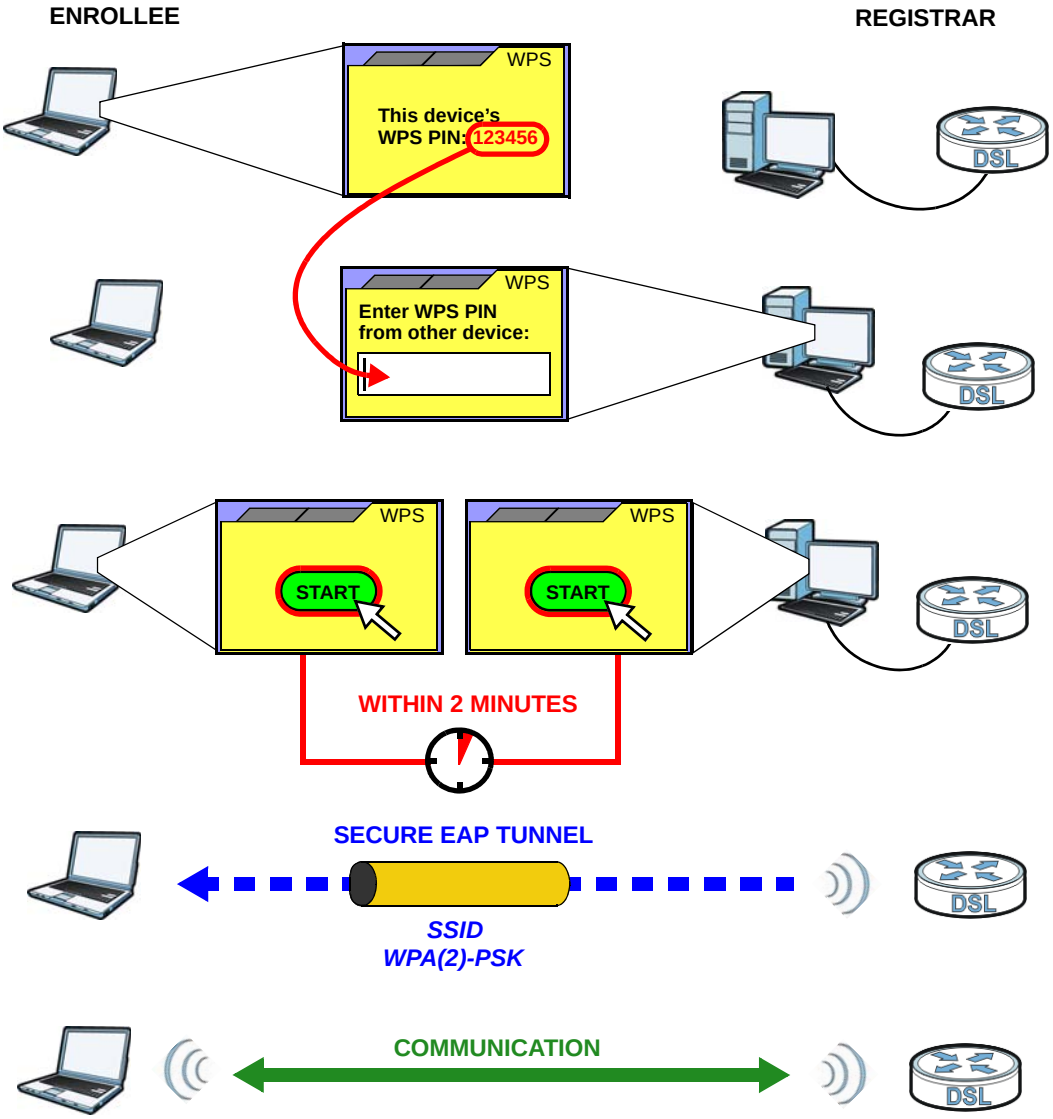
Take the following steps to set up a WPS connection between an access point or wireless router (referred to here as the AP) and a client device using the PIN method.

1. Ensure WPS is enabled on both devices.
2. Access the WPS section of the AP's configuration interface. See the device's User's Guide for how to do this.
3. Look for the client's WPS PIN; it will be displayed either on the device, or in the WPS section of the client's configuration interface (see the device's User's Guide for how to find the WPS PIN - for the ZyXEL Device, see Section 6.4 on page 115).
4. Enter the client's PIN in the AP's configuration interface.
5. If the client device's configuration interface has an area for entering another device's PIN, you can either enter the client's PIN in the AP, or enter the AP's PIN in the client - it does not matter which.
6. Start WPS on both devices within two minutes.
7. Use the configuration utility to activate WPS, not the push-button on the device itself.
8. On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

   If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 40 Example WPS Process: PIN Method

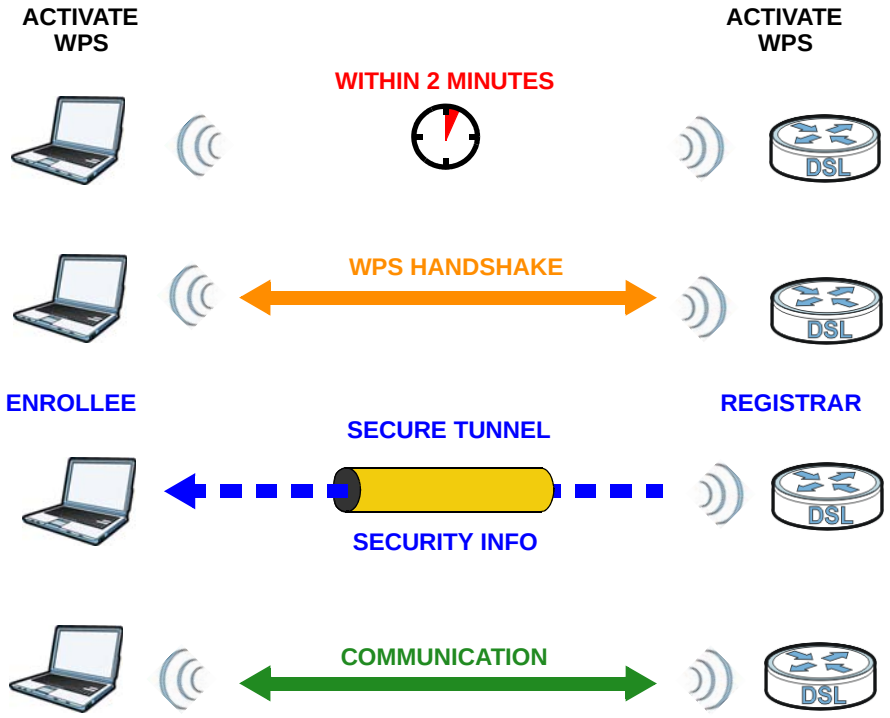


6.7.6.3 How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 41 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

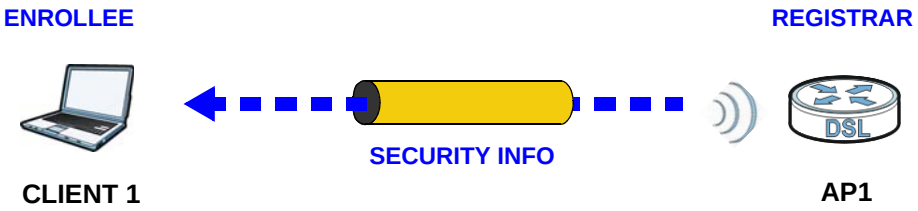
By default, a WPS devices is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

6.7.6.4 Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

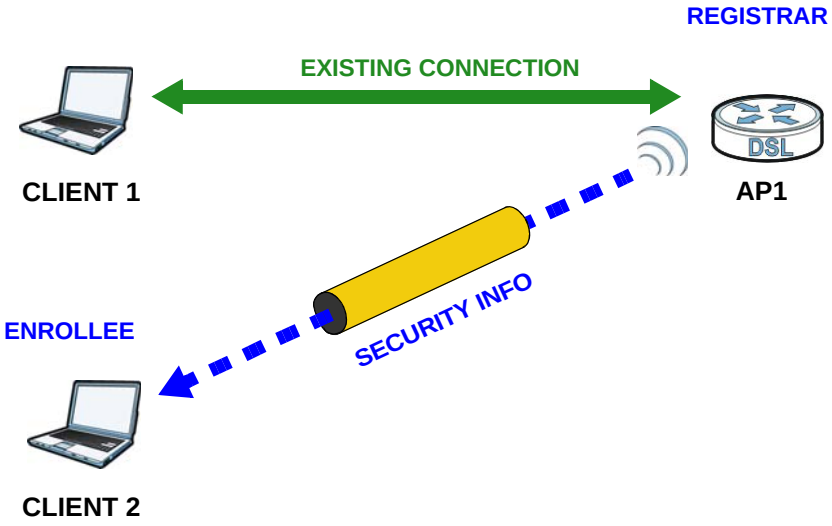
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 42 WPS: Example Network Step 1



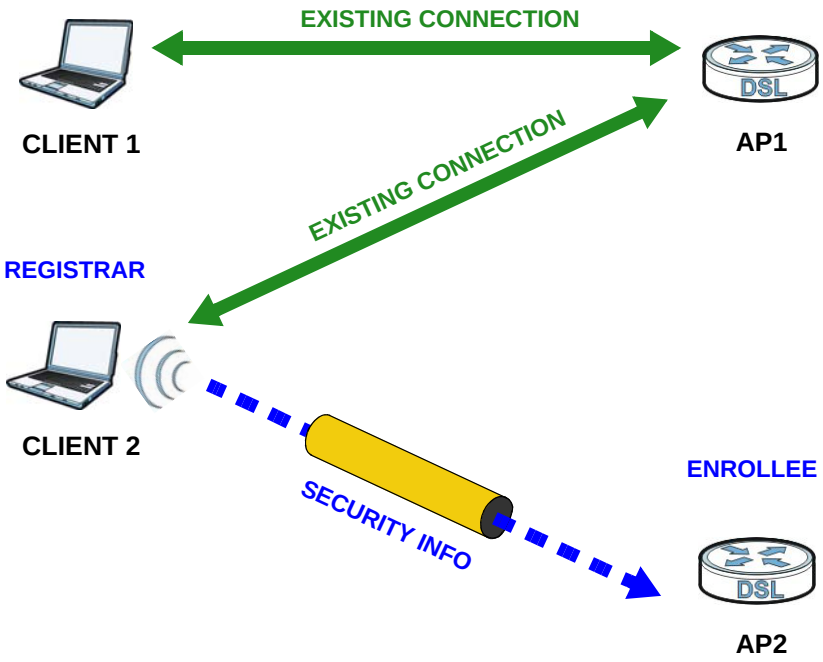
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 43 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 44 WPS: Example Network Step 3



6.7.6.5 Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).

- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the "correct" enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point's configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

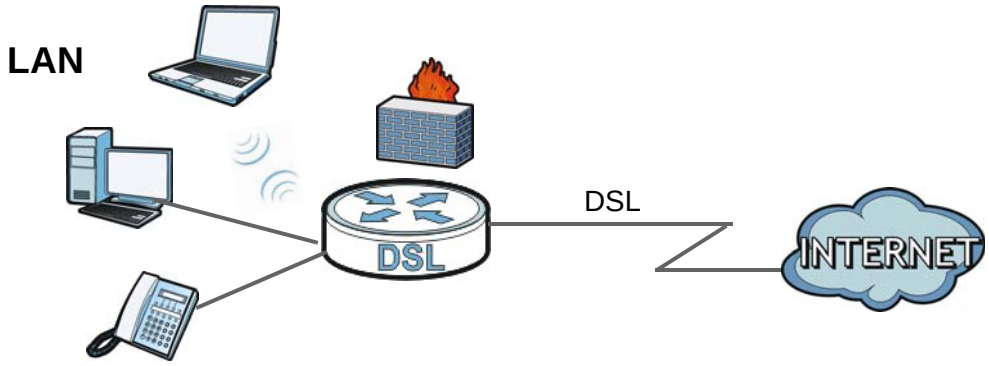
7

Home Networking

7.1 Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is usually located in one immediate area such as a building or floor of a building.

The LAN screens can help you configure a LAN DHCP server and manage IP addresses.



7.1.1 What You Can Do in this Chapter

- Use the **LAN IP** screen to set the LAN IP address, subnet mask, and DHCP settings (Section 7.2 on page 134).
- Use the **DHCP Server** screen to configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN (Section 7.3 on page 136).
- Use the **UPnP** screen to enable UPnP (Section 7.4 on page 137).
- Use the **File Sharing** screen to enable file-sharing server (Section 7.5 on page 138).
- Use the **Media Server** screen to enable media server (Section 7.6 on page 142).
- Use the **Printer Server** screen to enable the print server (Section 7.7 on page 143).

7.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

7.1.2.1 About LAN

IP Address

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number. This is known as an Internet Protocol address.

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows clients to obtain TCP/IP configuration at start-up from a server. This ZyXEL Device has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

DNS

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

7.1.2.2 About UPnP

How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

When a UPnP device joins a network, it announces its presence with a multicast message. For security reasons, the ZyXEL Device allows multicast messages on the LAN only.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports Internet Gateway Device (IGD) 1.0.

See Section 7.9 on page 148 for examples of installing and using UPnP.

7.1.2.3 About File Sharing

User Account

This gives you access to the file sharing server. It includes your user name and password.

Workgroup name

This is the name given to a set of computers that are connected on a network and share resources such as a printer or files. Windows automatically assigns the workgroup name when you set up a network.

Shares

When settings are set to default, each USB device connected to the ZyXEL Device is given a folder, called a “share”. If a USB hard drive connected to the ZyXEL Device has more than one partition, then each partition will be allocated a share. You can also configure a “share” to be a sub-folder or file on the USB device.

File Systems

A file system is a way of storing and organizing files on your hard drive and storage device. Often different operating systems such as Windows or Linux have different file systems. The file sharing feature on your ZyXEL Device supports File Allocation Table (FAT), FAT32, and New Technology File System (NTFS).

Common Internet File System

The ZyXEL Device uses Common Internet File System (CIFS) protocol for its file sharing functions. CIFS compatible computers can access the USB file storage devices connected to the ZyXEL Device. CIFS protocol is supported on Microsoft Windows, Linux Samba and other operating systems (refer to your systems specifications for CIFS compatibility).

7.1.2.4 About Media Server

Media Server

The media server feature lets anyone on your network play video, music, and photos from the ZyXEL Device (without having to copy them to another computer). The ZyXEL Device streams files to DLNA-compliant media clients without any configuration.

DLNA

The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network in order to make digital living easy and seamless. DLNA clients play files stored on DLNA servers.

7.1.2.5 About Printer Server

Print Server

This is a computer or other device which manages one or more printers, and which sends print jobs to each printer from the computer itself or other devices.

Operating System

An operating system (OS) is the interface which helps you manage a computer. Common examples are Microsoft Windows, Mac OS or Linux.

TCP/IP

TCP/IP (Transmission Control Protocol/ Internet Protocol) is a set of communications protocols that most of the Internet runs on.

Port

A port maps a network service such as http to a process running on your computer, such as a process run by your web browser. When traffic from the Internet is received on your computer, the port number is used to identify which process running on your computer it is intended for.

Line Printer Remote Protocol

The Line Printer Remote (LPR) Protocol is software that provides printer spooling and print-server features using TCP/IP to connect printers and computers on a network.

Supported OSs

Your operating system must support TCP/IP ports for printing and be compatible with the LPR protocol.

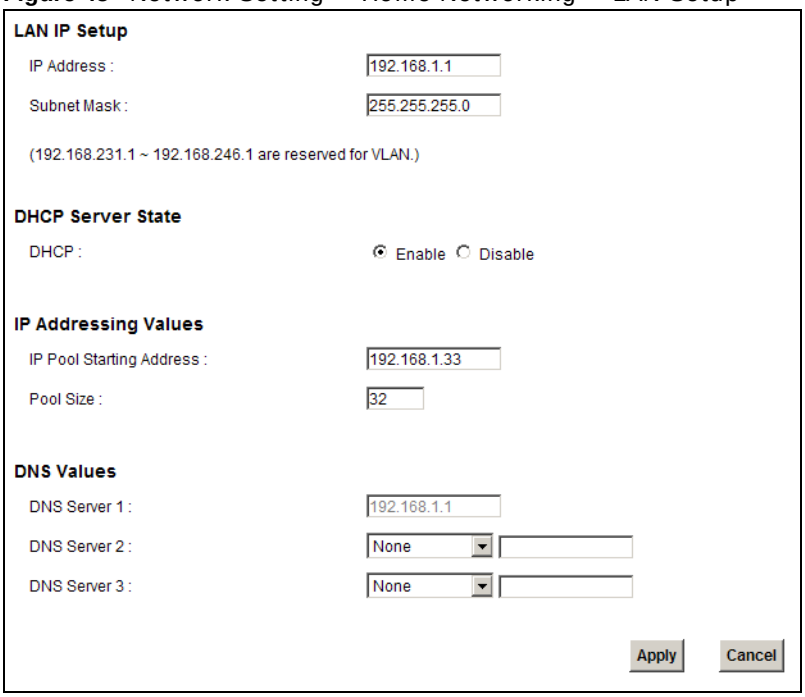
The following OSs support ZyXEL Device's printer sharing feature.

- Microsoft Windows 95, Windows 98 SE (Second Edition), Windows Me, Windows NT 4.0, Windows 2000, Windows XP or Macintosh OS X.

7.2 The LAN Setup Screen

Click **Network Setting > Home Networking** to open the **LAN Setup** screen. Use this screen to set the Local Area Network IP address and subnet mask of your ZyXEL Device and configure the DNS server information that the ZyXEL Device sends to the DHCP client devices on the LAN.

Figure 45 Network Setting > Home Networking > LAN Setup



The following table describes the fields on this screen.

Table 27 Network Setting > Home Networking > LAN Setup

LABEL	DESCRIPTION
LAN IP Setup	
IP Address	Enter the LAN IP address you want to assign to your ZyXEL Device in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask of your network in dotted decimal notation, for example 255.255.255.0 (factory default). Your ZyXEL Device automatically computes the subnet mask based on the IP address you enter, so do not change this field unless you are instructed to do so.
DHCP Server State	
DHCP	Select **Enable** to have your ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to LAN computers and other devices that are DHCP clients. If you select **Disable**, you need to manually configure the IP addresses of the computers and other devices on your LAN. When DHCP is used, the following fields need to be set.
IP Addressing Values	
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size, or count of the IP address pool.
DNS Values	

Table 27 Network Setting > Home Networking > LAN Setup (continued)

LABEL	DESCRIPTION
DNS Server 1-3	Select **From ISP** if your ISP dynamically assigns DNS server information (and the ZyXEL Device's WAN IP address). Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose **User-Defined**, but leave the IP address set to 0.0.0.0, **User-Defined** changes to **None** after you click **Apply**. If you set a second choice to **User-Defined**, and enter the same IP address, the second **User-Defined** changes to **None** after you click **Apply**. Select **None** if you do not want to configure DNS servers. You must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.3 The Static DHCP Screen

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

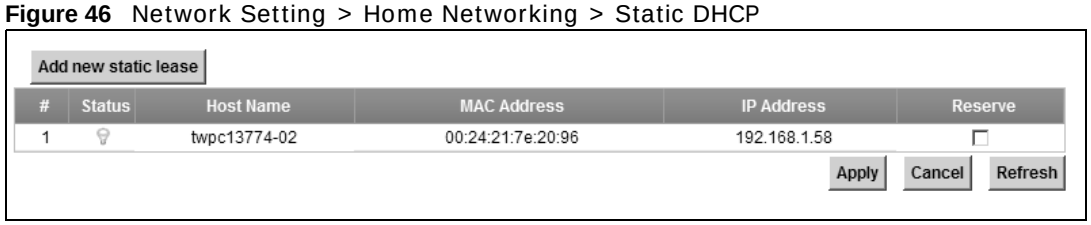
Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

7.3.1 Before You Begin

Find out the MAC addresses of your network devices if you intend to add them to the **Static DHCP** screen.

Use this screen to change your ZyXEL Device's static DHCP settings. Click **Network Setting > Home Networking > Static DHCP** to open the following screen.

Figure 46 Network Setting > Home Networking > Static DHCP



The following table describes the labels in this screen.

Table 28 Network Setting > Home Networking > Static DHCP

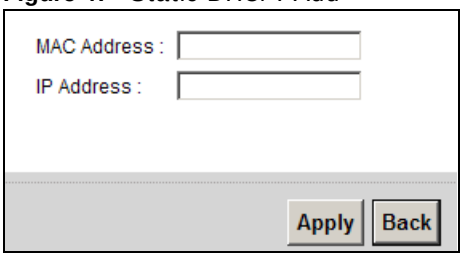
LABEL	DESCRIPTION
Add new static lease	Click this to add a new static DHCP entry.
#	This is the index number of the entry.
Status	This field displays whether the client is connected to the ZyXEL Device.
Host Name	This field displays the client host name.

Table 28 Network Setting > Home Networking > Static DHCP (continued)

LABEL	DESCRIPTION
MAC Address	The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal notation). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.
IP Address	This field displays the IP address relative to the # field listed above.
Reserve	Select the check box in the heading row to automatically select all check boxes or select the check box(es) in each entry to have the ZyXEL Device always assign the selected entry(ies)'s IP address(es) to the corresponding MAC address(es) (and host name(s)). You can select up to 128 entries in this table.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.
Refresh	Click **Refresh** to reload the DHCP table.

If you click **Add new static lease** in the **Static DHCP** screen, the following screen displays.

Figure 47 Static DHCP: Add



The following table describes the labels in this screen.

Table 29 Static DHCP: Add

LABEL	DESCRIPTION
MAC Address	Enter the MAC address of a computer on your LAN.
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

7.4 The UPnP Screen

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

See page 148 for more information on UPnP.

Use the following screen to configure the UPnP settings on your ZyXEL Device. Click **Network Setting > Home Networking > UPnP** to display the screen shown next.

Figure 48 Network Setting > Home Networking > UPnP



The following table describes the labels in this screen.

Table 30 Network Settings > Home Networking > UPnP

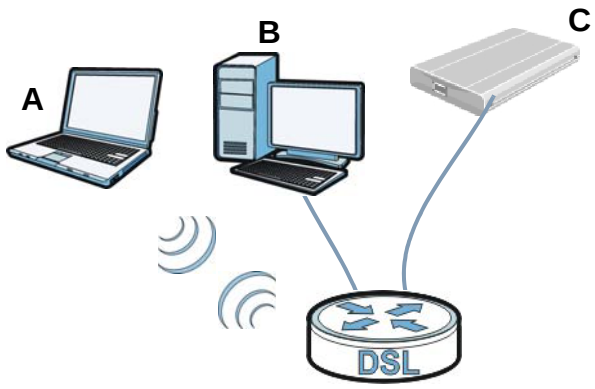
LABEL	DESCRIPTION
UPnP	Select **Enable** to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address (although you must still enter the password to access the web configurator).
Apply	Click **Apply** to save your changes.

7.5 The File Sharing Screen

You can share files on a USB memory stick or hard drive connected to your ZyXEL Device with users on your network.

The following figure is an overview of the ZyXEL Device's file server feature. Computers **A** and **B** can access files on a USB device (**C**) which is connected to the ZyXEL Device.

Figure 49 File Sharing Overview



The ZyXEL Device will not be able to join the workgroup if your local area network has restrictions set up that do not allow devices to join a workgroup. In this case, contact your network administrator.

7.5.1 Before You Begin

Make sure the ZyXEL Device is connected to your network and turned on.

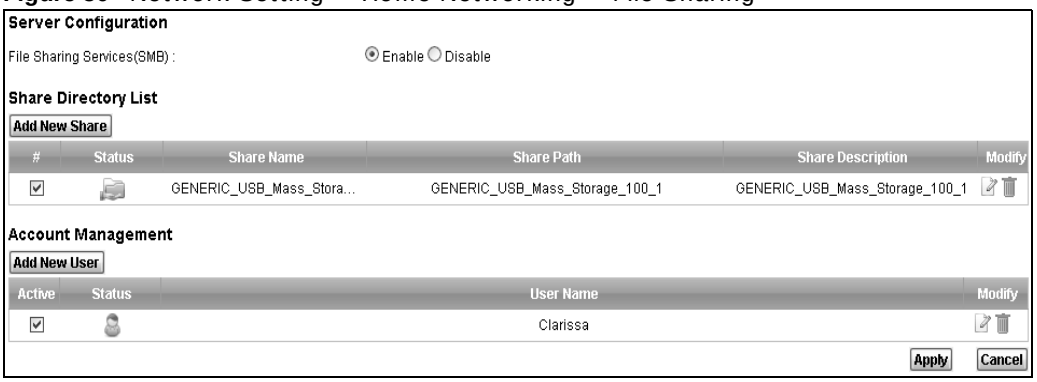
1 Connect the USB device to the ZyXEL Device's USB port. Make sure the ZyXEL Device is connected to your network.

2 The ZyXEL Device detects the USB device and makes its contents available for browsing. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.

Note: If your USB device cannot be detected by the ZyXEL Device, see troubleshooting for suggestions.

Use this screen to set up file sharing using the ZyXEL Device. To access this screen, click **Network Setting > Home Networking > File Sharing**.

Figure 50 Network Setting > Home Networking > File Sharing



Each field is described in the following table.

Table 31 Network Setting > Home Networking > File Sharing

LABEL	DESCRIPTION
Server Configuration	
File Sharing Services (SMB)	Select **Enable** to activate file sharing through the ZyXEL Device.
Share Directory List	
Add New Share	Click this to set up a new share.
#	Select the check box to make the share available to the network.
Status	This shows whether or not the share is available for sharing.
Share Name	This field displays the share name on the ZyXEL Device.
Share Path	This field displays the path for the share directories (folders) on the ZyXEL Device. These are the directories (folders) on your USB storage device.
Share Description	This field displays information about the share.
Modify	Click the **Edit** icon to change the settings of an existing share. Click the **Delete** icon to delete this share from the list.
Account Management. This table uses **Clarissa** as an example for **Username**. If no users have been created, these fields will appear empty.	

Table 31 Network Setting > Home Networking > File Sharing

LABEL	DESCRIPTION
Add New User	Click this only if you want to define a user name and a password required to access the share - see 7.5.3. Note: By default, everyone connected to the ZyXEL Device can access the share. You only need to create users if you wish to restrict access to the content on the share.
Active	Select the check box to allow this user to access shares on your network - see 7.5.3
Status	This shows whether or not the user is able to access shares on your network.
User Name	This field displays the users that have been added to the ZyXEL Device's Account Management screen
Modify	Click the **Edit** icon to change the settings of an existing user. Click the **Delete** icon to delete this user from the list.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

7.5.2 Add/Edit File Sharing

Use these screens to set up a new share or edit an existing share on the ZyXEL Device. Click **Add New share** in the **File Sharing** screen or click the **Edit** icon next to an existing share to change the settings.

Figure 51 File Sharing: Add Share



Each field is described in the following table.

Table 32 File Sharing: Add New Share

LABEL	DESCRIPTION
Volume	Select the USB storage device that you want to add as a share in the ZyXEL Device. The device will be selected automatically unless your USB device is partitioned into two or more volumes.
Share Path	Manually enter the file path for the share, or click the **Browse** button and select the folder that you want to add as a share.
Description	You can either enter a short description of the share, or leave this field blank.

Table 32 File Sharing: Add New Share

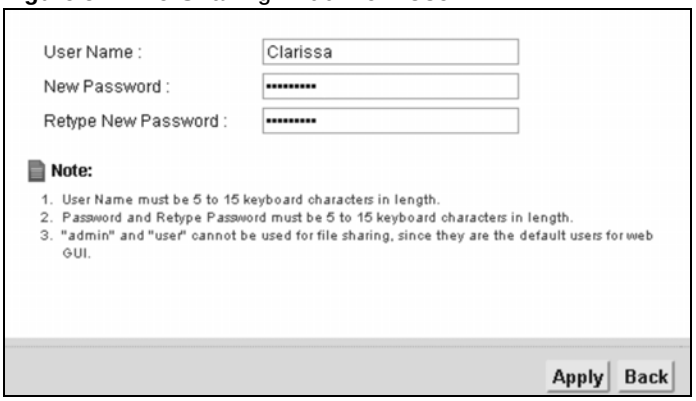
LABEL	DESCRIPTION
Access Level	Select **Public** to make the share available to all users on your network. This is the default option. Select **Security** if you wish define usernames and passwords required to access a specific share - see 7.5.3 to create users. If you select this option, two lists will appear below and you must select from those lists which users can access the share
Available Users	This list shows all the users that you have created on the ZyXEL Device - see 7.5.3 to create users
Allow Users	This list shows the users from the list **Available Users** that you have granted access to the ZyXEL Device.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

Click on the **Edit** icon under the **Modify** label to change a share's settings.

7.5.3 Add New User

Use these screens to set up a new user or edit an existing user on the ZyXEL Device. Click **Add New User** in the **File Sharing** screen or click the **Edit** icon next to an existing user to change the settings. You can only edit the user's name while on the Add New User screen.

Figure 52 File Sharing: Add New User


User Name :
Clarissa
New Password :
Retype New Password :
Note:
1. User Name must be 5 to 15 keyboard characters in length.
2. Password and Retype Password must be 5 to 15 keyboard characters in length.
3. "admin" and "user" cannot be used for file sharing, since they are the default users for web GUI.
Apply
Back

Each field is described in the following table.

Table 33 File Sharing: Add New User

LABEL	DESCRIPTION
User Name	Enter a user name that will be allowed to access shares. It must be 5 to 15 characters long. Only letters and numbers allowed.
New Password	Enter the password used to access the share. It must be 5 to 15 characters long. Only letters and numbers are allowed. The password is case sensitive.
Retype New Password	Retype the password that you entered above
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen.

Click on the **Edit** icon under the **Modify** label to change a user's settings.

7.6 The Media Server Screen

You can set up your ZyXEL Device to act as a media server to provide media (like video) to DLNA-compliant players, such as Windows Media Player, ZyXEL DMAs (Digital Media Adapters), Xboxes or PS3s. The media server and the clients must have IP addresses in the same subnet.

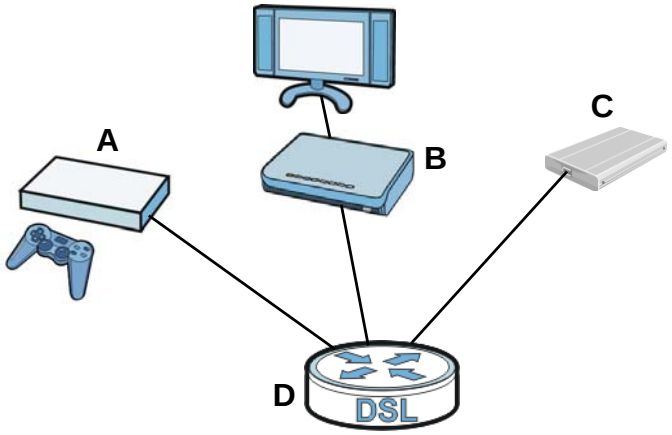
The ZyXEL Device media server enables you to:

- Publish all shares for everyone to play media files in the USB storage device connected to the ZyXEL Device.
- Use hardware-based media clients like the DMA-2500 to play the files.

Note: Anyone on your network can play the media files in the published shares. No user name and password or other form of security is used. The media server is enabled by default with the video, photo, and music shares published.

The following figure is an overview of the ZyXEL Device's media server feature. DLNA devices **A** and **B** can access and play files on a USB device (**C**) which is connected to the ZyXEL Device (**D**).

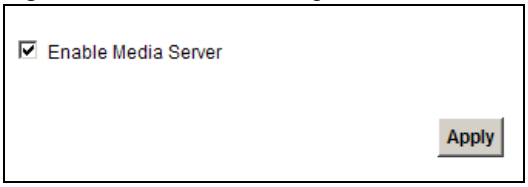
Figure 53 Media Server Overview



7.6.1 The Media Server Screen

Use this screen to have the ZyXEL Device work as a media server. To access this screen, click **Network Setting > Home Networking > Media Server**.

Figure 54 Network Setting > Home Networking > Media Server



Each field is described in the following table.

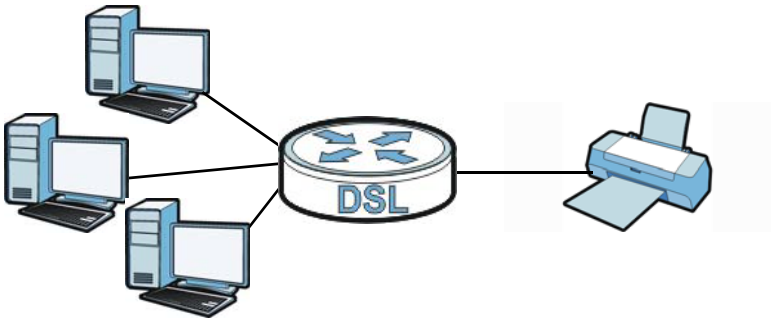
Table 34 Network Setting > Home Networking > Media Server

LABEL	DESCRIPTION
Enable Media Server	Select this to have the ZyXEL Device function as a DLNA-compliant media server.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.

7.7 The Print Server Screen

The ZyXEL Device allows you to share a USB printer on your LAN. You can do this by connecting a USB printer the USB port on the ZyXEL Device and then configuring a TCP/IP port on the computers connected to your network.

Figure 55 Sharing a USB Printer



7.7.1 Before You Begin

To configure the print server you need the following:

- Your ZyXEL Device must be connected to your computer and any other devices on your network. The USB printer must be connected to your ZyXEL Device.
- A USB printer with the driver already installed on your computer.
- The computers on your network must have the printer software already installed before they can create a TCP/IP port for printing via the network. Follow your printer manufacturers instructions on how to install the printer software on your computer.

Note: Your printer's installation instructions may ask that you connect the printer to your computer. Connect your printer to the ZyXEL Device instead.

Use this screen to enable or disable sharing of a USB printer via your ZyXEL Device.

To access this screen, click **Network Setting > Home Networking > Printer Server**.

Figure 56 Network Setting > Home Networking > Printer Server



The following table describes the labels in this menu.

Table 35 Network Setting > Home Networking > Print Server

LABEL	DESCRIPTION
Printer Server	Select **Enable** to have the ZyXEL Device share a USB printer.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

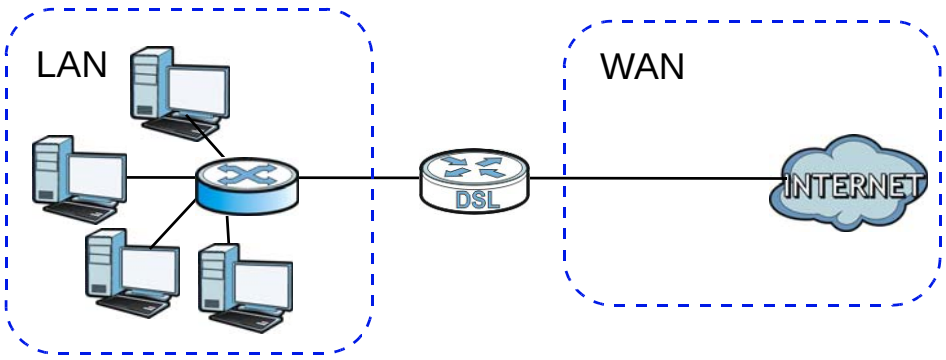
7.8 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

LANs, WANs and the ZyXEL Device

The actual physical connection determines whether the ZyXEL Device ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 57 LAN and WAN IP Addresses



DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the ZyXEL Device as a DHCP server or disable it. When configured as a server, the ZyXEL Device provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

IP Pool Setup

The ZyXEL Device is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

LAN TCP/IP

The ZyXEL Device has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the ZyXEL Device. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your ZyXEL Device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, “Address Allocation for Private Internets” and RFC 1466, “Guidelines for Management of IP Address Space”.

ZyXEL Device Print Server Compatible USB Printers

The following is a list of USB printer models compatible with the ZyXEL Device print server.

Table 36 Compatible USB Printers

BRAND	MODEL
Brother	MFC7420
CANON	BJ F9000
CANON	i320
CANON	PIXMA MP450
CANON	PIXMA MP730
CANON	PIXMA MP780
CANON	PIXMA MP830
CANON	PIXUS ip2500
CANON	PIXMA ip4200
CANON	PIXMA ip5000
CANON	PIXUS 990i
EPSON	CX3500
EPSON	CX3900
EPSON	EPL-5800
EPSON	EPL-6200L
EPSON	LP-2500
EPSON	LP-8900
EPSON	RX 510
EPSON	RX 530
EPSON	Stylus 830U
EPSON	Stylus 1270
EPSON	Stylus C43UX
EPSON	Stylus C60

Table 36 Compatible USB Printers (continued)

BRAND	MODEL
EPSON	Stylus Color 670
HP	Deskjet 5550
HP	Deskjet 5652
HP	Deskjet 830C
HP	Deskjet 845C
HP	Deskjet 1125C
HP	Deskjet 1180C
HP	Deskjet 1220C
HP	Deskjet F4185
HP	Laserjet 1022
HP	Laserjet 1200
HP	Laserjet 2200D
HP	Laserjet 2420
HP	Color Laserjet 1500L
HP	Laserjet 3015
HP	Officejet 4255
HP	Officejet 5510
HP	Officejet 5610
HP	Officejet 7210
HP	Officejet Pro L7380
HP	Photosmart 2610
HP	Photosmart 3110
HP	Photosmart 7150
HP	Photosmart 7830
HP	Photosmart C5280
HP	Photosmart D5160
HP	PSC 1350
HP	PSC 1410
IBM	Infoprint 1332
LEXMARK	Z55
LEXMARK	Z705

Table 36 Compatible USB Printers (continued)

BRAND	MODEL
OKI	B4350
SAMSUNG	ML-1710
SAMSUNG	SCX-4016

7.9 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

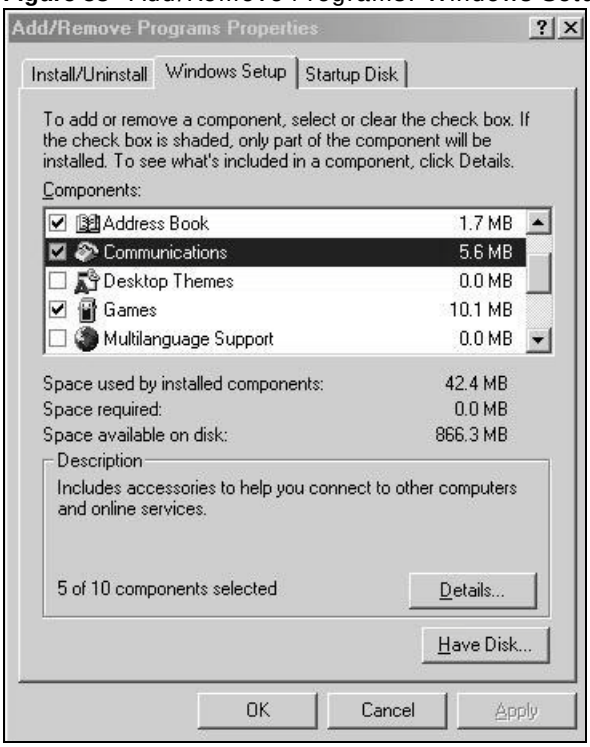
Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

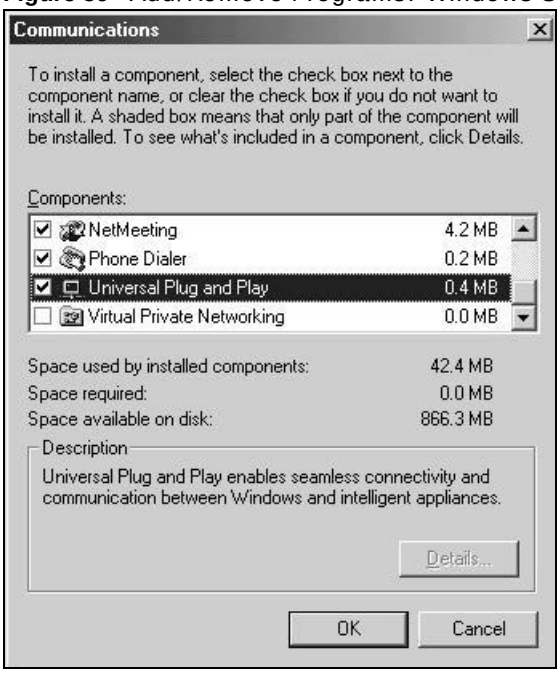
2 Click the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 58 Add/Remove Programs: Windows Setup: Communication


Add/Remove Programs Properties
Install/Uninstall
Windows Setup
Startup Disk
To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.
Components:
Address Book 1.7 MB
Communications 5.6 MB
Desktop Themes 0.0 MB
Games 10.1 MB
Multilanguage Support 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Includes accessories to help you connect to other computers and online services.
5 of 10 components selected
Details...
Have Disk...
OK
Cancel
Apply

3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 59 Add/Remove Programs: Windows Setup: Communication: Components


Communications
To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
NetMeeting 4.2 MB
Phone Dialer 0.2 MB
Universal Plug and Play 0.4 MB
Virtual Private Networking 0.0 MB
Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB
Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.
Details...
OK
Cancel

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

Installing UPnP in Windows XP

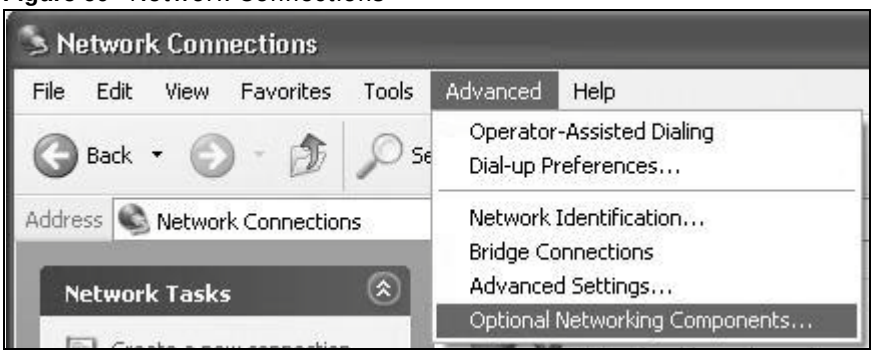
Follow the steps below to install the UPnP in Windows XP.

1 Click **Start** and **Control Panel**.

2 Double-click **Network Connections**.

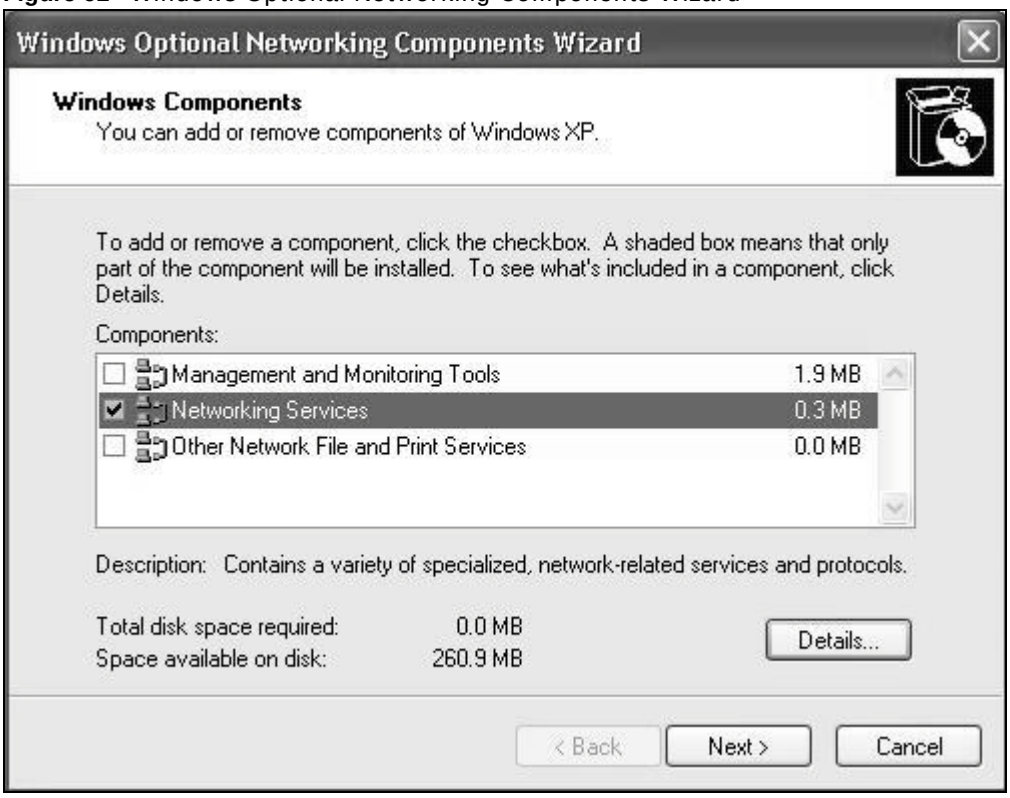
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.

Figure 60 Network Connections



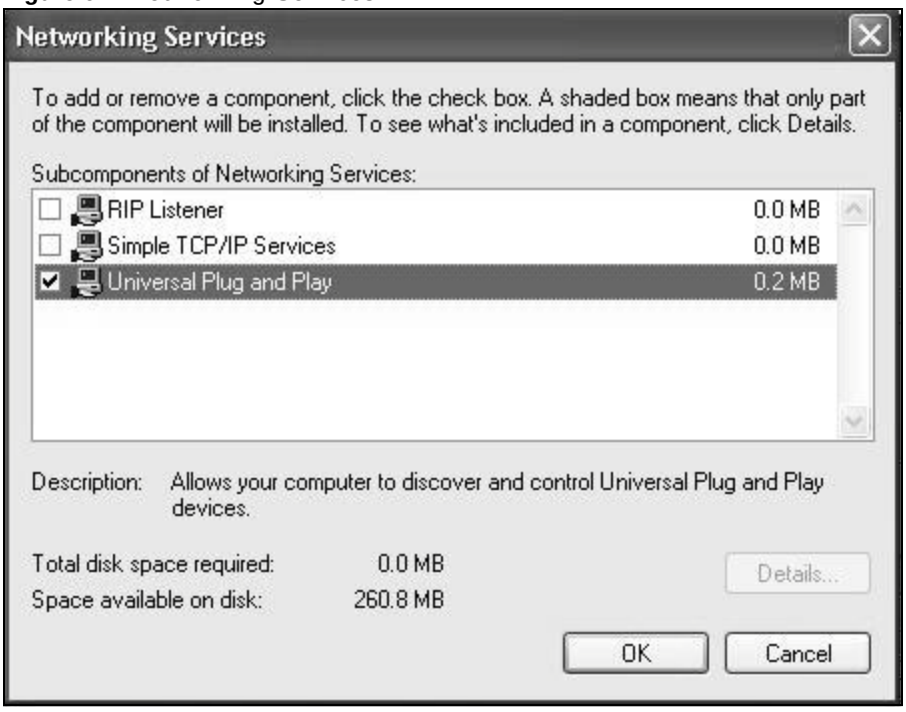
4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 61 Windows Optional Networking Components Wizard


Windows Optional Networking Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Management and Monitoring Tools 1.9 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 0.0 MB
Space available on disk: 260.9 MB
Details...
< Back
Next >
Cancel

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 62 Networking Services


Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
RIP Listener 0.0 MB
Simple TCP/IP Services 0.0 MB
Universal Plug and Play 0.2 MB
Description: Allows your computer to discover and control Universal Plug and Play devices.
Total disk space required: 0.0 MB
Space available on disk: 260.8 MB
Details...
OK
Cancel

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

7.10 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL Device.

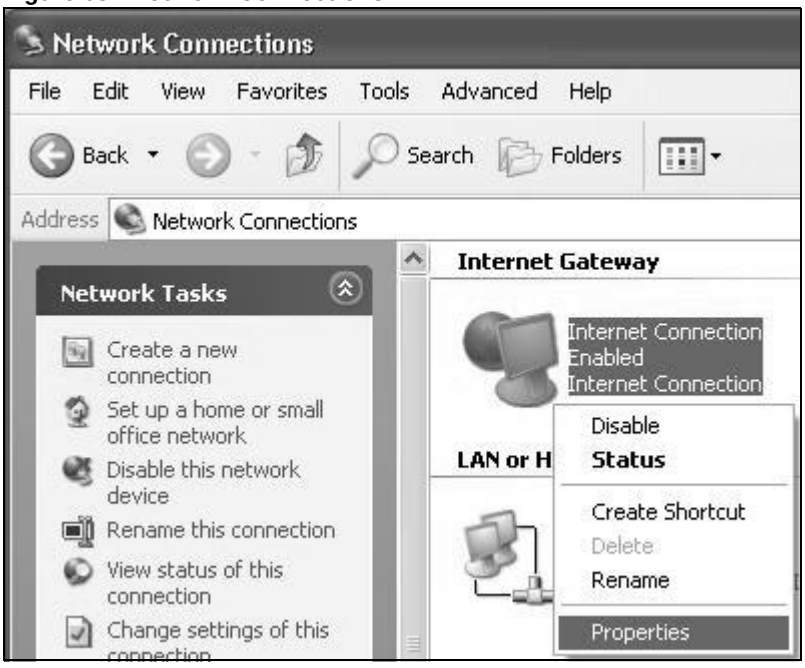
Make sure the computer is connected to a LAN port of the ZyXEL Device. Turn on your computer and the ZyXEL Device.

Auto-discover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

2 Right-click the icon and select **Properties**.

Figure 63 Network Connections



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 64 Internet Connection Properties


Internet Connection Properties
General
Connect to the Internet using:
Internet Connection
This connection allows you to connect to the Internet through a shared connection on another computer.
Settings...
Show icon in notification area when connected
OK
Cancel

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 65 Internet Connection Properties: Advanced Settings

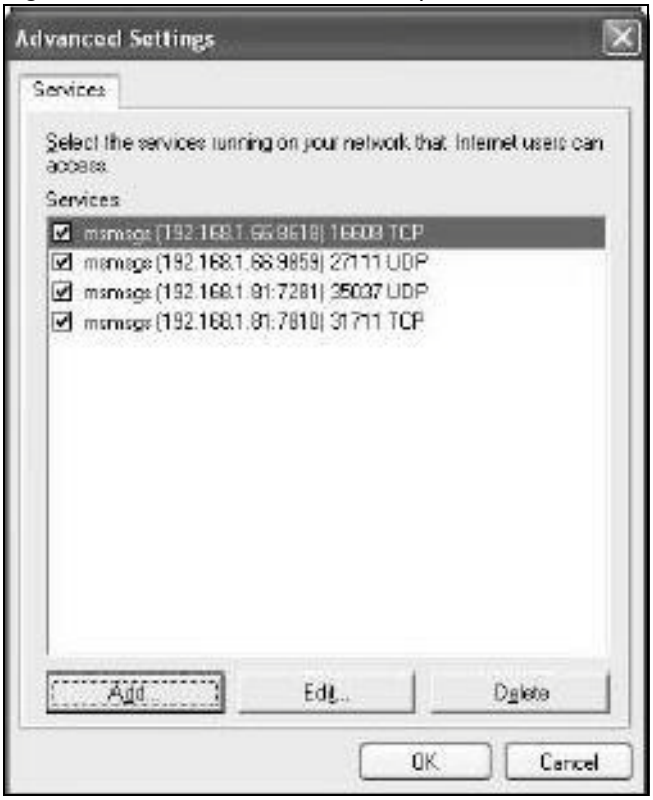
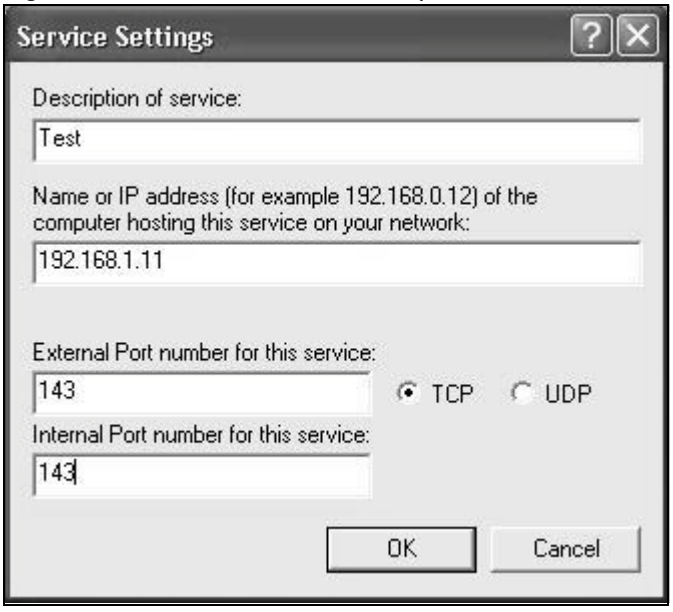


Figure 66 Internet Connection Properties: Advanced Settings: Add



5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

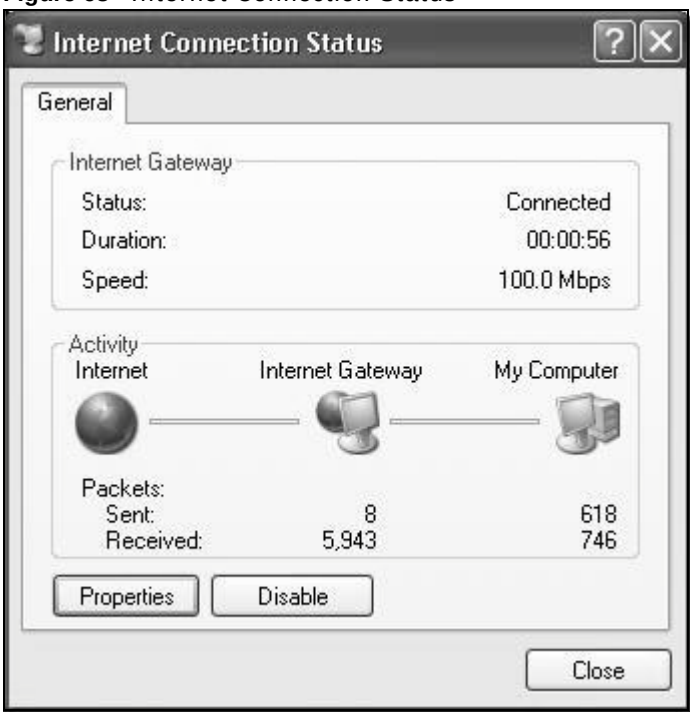
6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 67 System Tray Icon



7 Double-click on the icon to display your current Internet connection status.

Figure 68 Internet Connection Status



Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This comes helpful if you do not know the IP address of the ZyXEL Device.

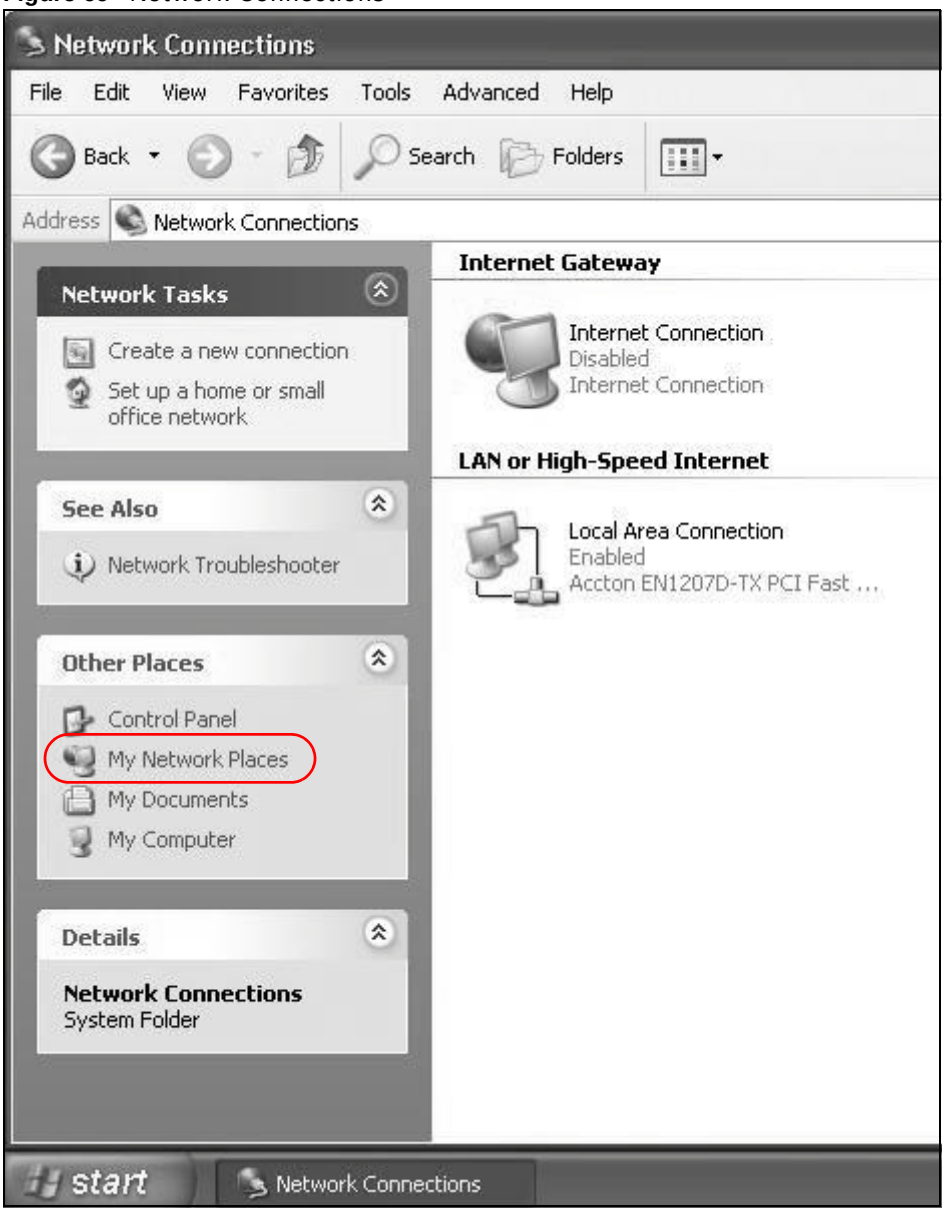
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

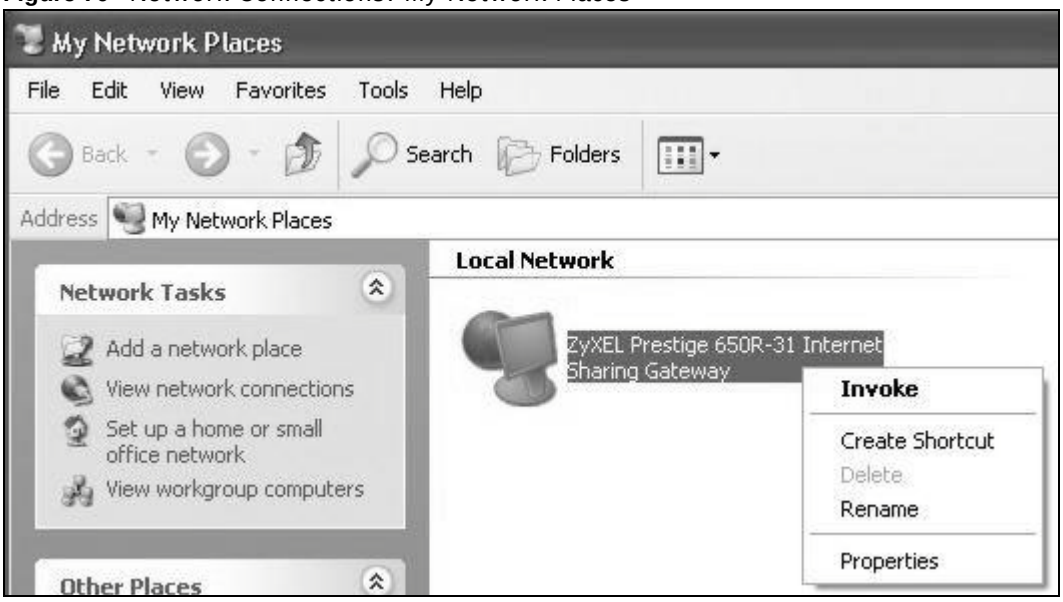
Figure 69 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.

Figure 70 Network Connections: My Network Places



6 Right-click on the icon for your ZyXEL Device and select **Properties**. A properties window displays with basic information about the ZyXEL Device.

Figure 71 Network Connections: My Network Places: Properties: Example



8

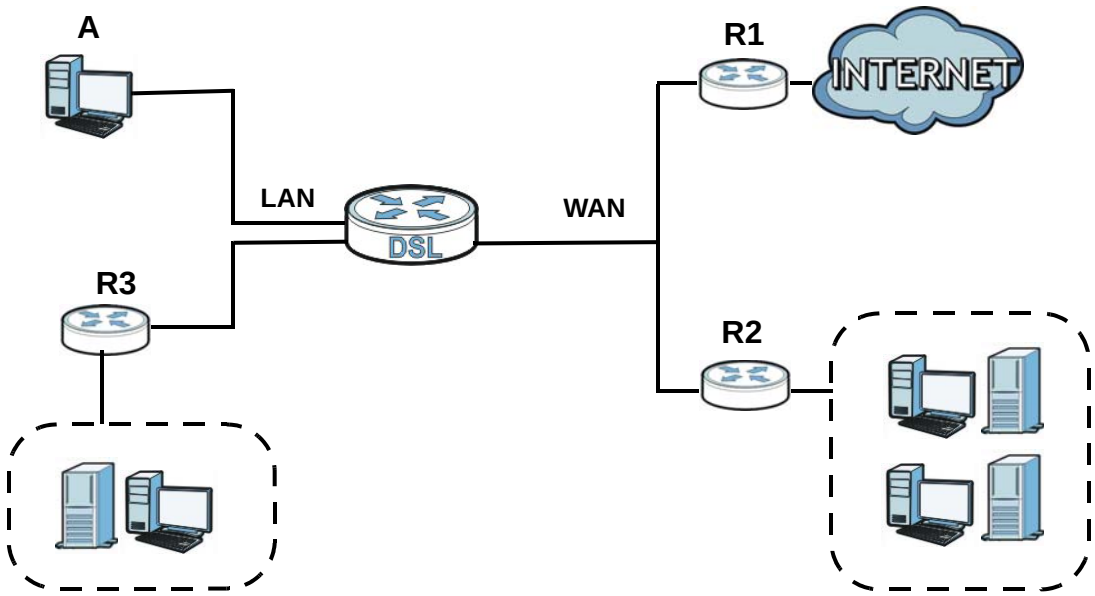
Routing

8.1 Overview

The ZyXEL Device usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the ZyXEL Device send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the ZyXEL Device's LAN interface. The ZyXEL Device routes most traffic from **A** to the Internet through the ZyXEL Device's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the LAN.

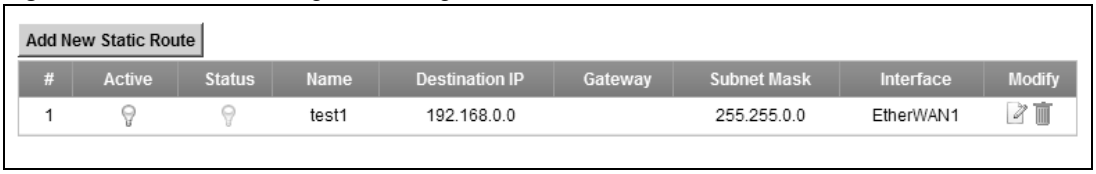
Figure 72 Example of Static Routing Topology



8.2 Configuring Static Route

Use this screen to view and configure IP static routes on the ZyXEL Device. Click **Network Setting > Routing** to open the following screen.

Figure 73 Network Setting > Routing


Add New Static Route
Active Status Name Destination IP Gateway Subnet Mask Interface Modify
1 test1 192.168.0.0 255.255.0.0 EtherWAN1

The following table describes the labels in this screen.

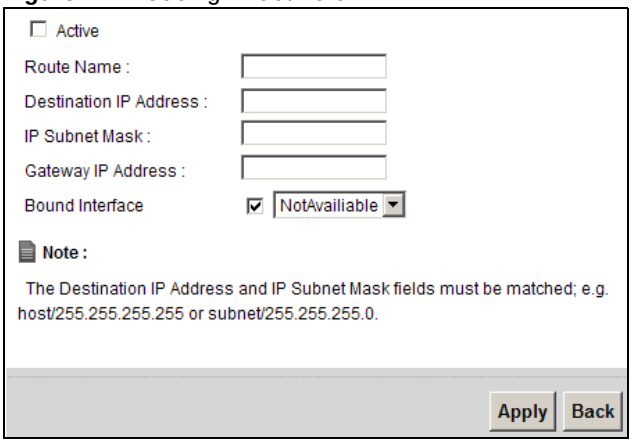
Table 37 Network Setting > Routing

LABEL	DESCRIPTION
Add New Static Route	Click this to set up a new static route on the ZyXEL Device.
#	This is the number of an individual static route.
Active	This indicates whether the rule is active or not. A yellow bulb signifies that this static route is active. A gray bulb signifies that this static route is not active.
Status	This shows whether the static route is currently in use or not. A yellow bulb signifies that this static route is in use. A gray bulb signifies that this static route is not in use.
Name	This is the name that describes or identifies this route.
Destination IP	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Subnet Mask	This parameter specifies the IP network subnet mask of the final destination.
Interface	This is the WAN interface through which the traffic is routed.
Modify	Click the **Edit** icon to go to the screen where you can set up a static route on the ZyXEL Device. Click the **Delete** icon to remove a static route from the ZyXEL Device.

8.2.1 Add/Edit Static Route

Click **add new Static Route** in the **Routing** screen or click the **Edit** icon next to a rule. The following screen appears. Use this screen to configure the required information for a static route.

Figure 74 Routing: Add/Edit



The following table describes the labels in this screen.

Table 38 Routing: Add/Edit

LABEL	DESCRIPTION
Active	Click this to activate this static route.
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	You can decide if you want to forward packets to a gateway IP address or a bound interface. If you want to configure **Gateway IP Address**, enter the IP address of the next-hop gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Bound Interface	You can decide if you want to forward packets to a gateway IP address or a bound interface. If you want to configure **Bound Interface**, select the check box and choose an interface through which the traffic is sent. You must have the WAN interface(s) already configured in the **Broadband** screen.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

9

DNS Route

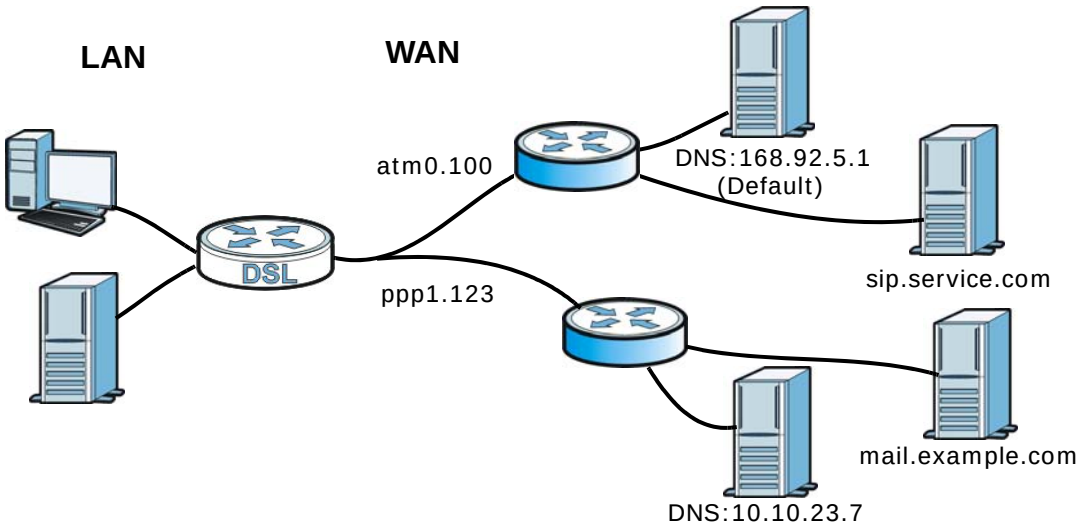
9.1 Overview

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it.

In addition to the system DNS server(s), each WAN interface (service) is set to have its own static or dynamic DNS server list. You can configure a DNS static route to forward DNS queries for certain domain names through a specific WAN interface to its DNS server(s). The ZyXEL Device uses a system DNS server (in the order you specify in the **Broadband** screen) to resolve domain names that do not match any DNS routing entry. After the ZyXEL Device receives a DNS reply from a DNS server, it creates a new entry for the resolved IP address in the routing table.

In the following example, the DNS server 168.92.5.1 obtained from the WAN interface atm0.100 is set to be the system DNS server. The DNS server 10.10.23.7 is obtained from the WAN interface ppp1.123. You configure a DNS route for *example.com to have the ZyXEL Device forward DNS requests for the domain name mail.example.com through the WAN interface ppp1.123 to the DNS server 10.10.23.7.

Figure 75 Example of DNS Routing Topology



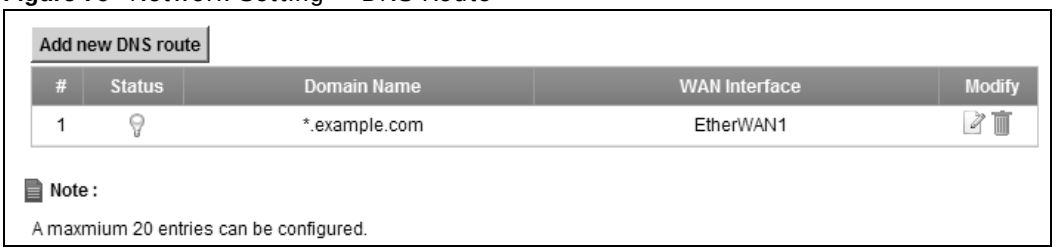
9.1.1 What You Can Do in this Chapter

The **DNS Route** screens let you view and configure DNS routes on the ZyXEL Device (Section 9.2 on page 162).

9.2 The DNS Route Screen

The **DNS Route** screens let you view and configure DNS routes on the ZyXEL Device. Click **Network Setting > DNS Route** to open the **DNS Route** screen.

Figure 76 Network Setting > DNS Route


Add new DNS route
Status Domain Name WAN Interface Modify
1 *.example.com EtherWAN1
Note :
A maxmium 20 entries can be configured.

The following table describes the labels in this screen.

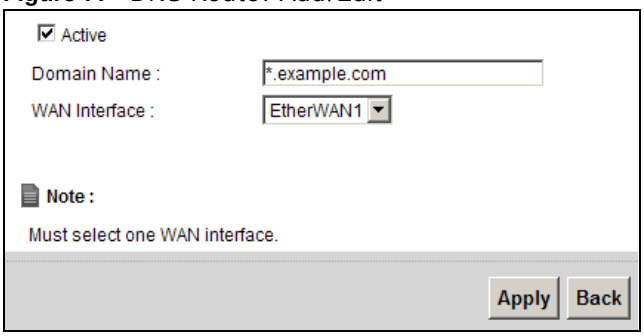
Table 39 Network Setting > DNS Route

LABEL	DESCRIPTION
Add new DNS route	Click this to create a new entry.
#	This is the number of an individual DNS route.
Status	This shows whether the DNS route is currently in use or not. A yellow bulb signifies that this DNS route is in use. A gray bulb signifies that this DNS route is not in use.
Domain Name	This is the domain name to which the DNS route applies.
WAN Interface	This is the WAN interface through which the matched DNS request is routed.
Modify	Click the **Edit** icon to configure a DNS route on the ZyXEL Device. Click the **Delete** icon to remove a DNS route from the ZyXEL Device.

9.2.1 Add/Edit DNS Route Edit

Click **Add new DNS route** in the **DNS Route** screen or the **Edit** icon next to an existing DNS route. Use this screen to configure the required information for a DNS route.

Figure 77 DNS Route: Add/Edit



The following table describes the labels in this screen.

Table 40 DNS Route: Add/Edit

LABEL	DESCRIPTION
Active	Select this to activate this DNS route.
Domain Name	Enter the domain name you want to resolve. You can use the wildcard character, an "*" (asterisk) as the left most part of a domain name, such as *.example.com. The ZyXEL Device forwards DNS queries for any domain name ending in example.com to the WAN interface specified in this route.
WAN Interface	Select a WAN interface through which the matched DNS query is sent. You must have the WAN interface(s) already configured in the **Broadband** screen.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to exit this screen without saving.

10

Quality of Service (QoS)

10.1 Overview

This chapter discusses the ZyXEL Device's **QoS** screens. Use these screens to set up your ZyXEL Device to use QoS for traffic management.

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to control the use of bandwidth. QoS allows the ZyXEL Device to group and prioritize application traffic and fine-tune network performance.

Without QoS, all traffic data is equally likely to be dropped when the network is congested. This can cause a reduction in network performance and make the network inadequate for time-critical application such as video-on-demand.

The ZyXEL Device assigns each packet a priority and then queues the packet accordingly. Packets assigned a high priority are processed more quickly than those with low priority if there is congestion, allowing time-sensitive applications to flow more smoothly. Time-sensitive applications include both those that require a low level of latency (delay) and a low level of jitter (variations in delay) such as Internet gaming, and those for which jitter alone is a problem such as Internet radio or streaming video.

10.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable QoS, set the bandwidth, and allow the ZyXEL Device to automatically assign priority to upstream traffic according to the IEEE 802.1p priority level, IP precedence or packet length (Section 10.2 on page 166).
- Use the **Queue Setup** screen to configure QoS queue assignment (Section 10.3 on page 167).
- Use the **Class Setup** screen to set up classifiers to sort traffic into different flows and assign priority and define actions to be performed for a classified traffic flow (Section 10.4 on page 169).
- Use the **Monitor** screen to view the ZyXEL Device's QoS-related packet statistics (Section 10.5 on page 173).

10.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

QoS versus Cos

QoS is used to prioritize source-to-destination traffic flows. All packets in the same flow are given the same priority. CoS (class of service) is a way of managing traffic in a network by grouping similar types of traffic together and treating each type as a class. You can use CoS to give different priorities to different packet types.

CoS technologies include IEEE 802.1p layer 2 tagging and DiffServ (Differentiated Services or DS). IEEE 802.1p tagging makes use of three bits in the packet header, while DiffServ is a new protocol and defines a new DS field, which replaces the eight-bit ToS (Type of Service) field in the IP header.

Tagging and Marking

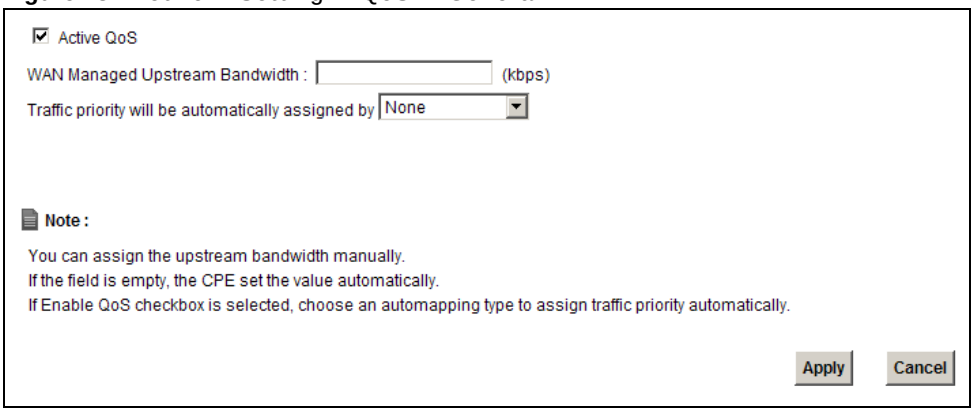
In a QoS class, you can configure whether to add or change the DSCP (DiffServ Code Point) value, IEEE 802.1p priority level and VLAN ID number in a matched packet. When the packet passes through a compatible network, the networking device, such as a backbone switch, can provide specific treatment or service based on the tag or marker.

10.2 The QoS General Screen

Use this screen to enable or disable QoS, set the bandwidth, and select to have the ZyXEL Device automatically assign priority to upstream traffic according to the IEEE 802.1p priority level, IP precedence or packet length.

Click **Network Setting > QoS** to open the **General** screen.

Figure 78 Network Setting > QoS > General


Active QoS
WAN Managed Upstream Bandwidth :
(kbps)
Traffic priority will be automatically assigned by
None
Note :
You can assign the upstream bandwidth manually.
If the field is empty, the CPE set the value automatically.
If Enable QoS checkbox is selected, choose an automapping type to assign traffic priority automatically.
Apply
Cancel

The following table describes the labels in this screen.

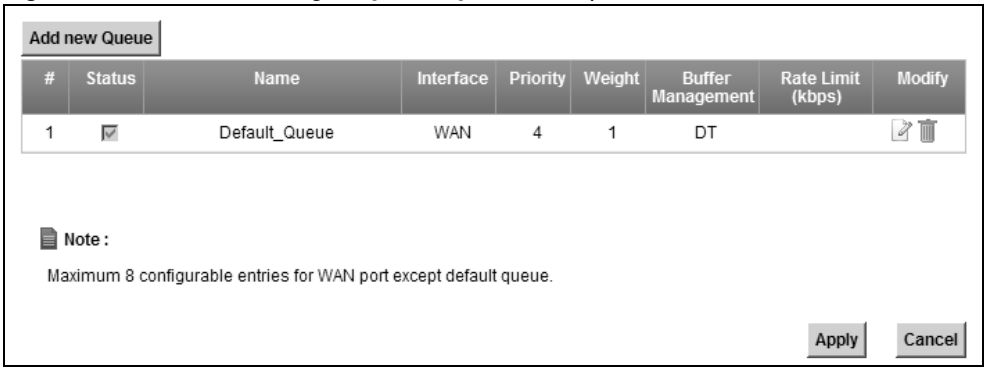
Table 41 Network Setting > QoS > General

LABEL	DESCRIPTION
Active QoS	Select the check box to turn on QoS to improve your network performance. You can give priority to traffic that the ZyXEL Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.
WAN Managed Upstream Bandwidth	Enter the amount of bandwidth for the WAN interface that you want to allocate using QoS. The recommendation is to set this speed to match the interface's actual transmission speed. For example, set the WAN interface speed to 1200 kbps if your Internet connection has an upstream transmission speed of 100 Mbps. Setting this number higher than the interface's actual transmission speed will stop lower priority traffic from being sent if higher priority traffic uses all of the actual bandwidth. If you set this number lower than the interface's actual transmission speed, the ZyXEL Device will not use some of the interface's available bandwidth. Leave this field blank to have the ZyXEL Device set this value automatically.
Traffic priority will be automatically assigned by	This field is ignored if upstream traffic matches a class you configured in the **Class Setup** screen. If you select **Ethernet Priority**, **IP Precedence** or **Packet Length** and traffic does not match a class configured in the **Class Setup** screen, the ZyXEL Device assigns priority to unmatched traffic based on the IEEE 802.1p priority level, IP precedence or packet length. See Section 10.6.1 on page 174 for more information.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.3 The Queue Setup Screen

Use this screen to configure QoS queue assignment. Click **Network Setting > QoS > Queue Setup** to open the screen as shown next.

Figure 79 Network Setting > QoS > Queue Setup


Add new Queue
Status Name Interface Priority Weight Buffer Management Rate Limit (kbps) Modify
1 Default_Queue WAN 4 1 DT
Note :
Maximum 8 configurable entries for WAN port except default queue.
Apply
Cancel

The following table describes the labels in this screen.

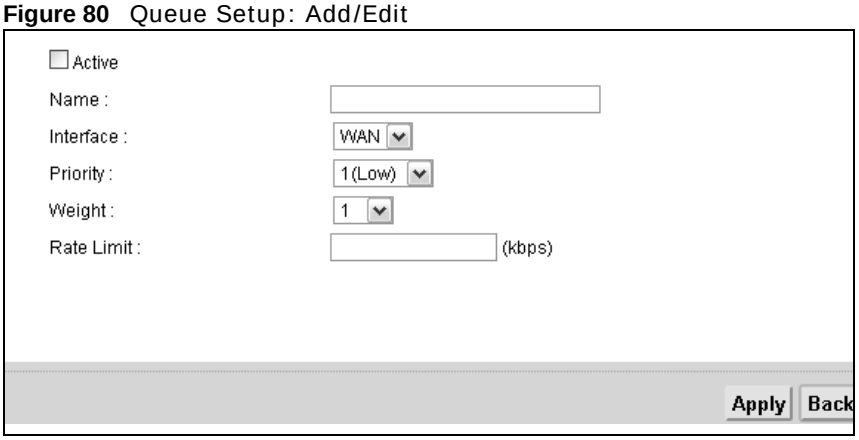
Table 42 Network Setting > QoS > Queue Setup

LABEL	DESCRIPTION
Add new Queue	Click this to create a new entry.
#	This is the index number of this entry.
Status	Select the check box to enable the queue.
Name	This shows the descriptive name of this queue.
Interface	This shows the name of the ZyXEL Device's interface through which traffic in this queue passes.
Priority	This shows the priority of this queue.
Weight	This shows the weight of this queue.
Buffer Management	This shows the queue management algorithm used by the ZyXEL Device.
Rate Limit (kbps)	This shows the maximum transmission rate allowed for traffic on this queue.
Modify	Click the **Edit** icon to edit the queue. Click the **Delete** icon to delete an existing queue. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.3.1 Add/Edit a QoS Queue

Use this screen to configure a queue. Click **Add new queue** in the **Queue Setup** screen or the **Edit** icon next to an existing queue.

Figure 80 Queue Setup: Add/Edit



The following table describes the labels in this screen.

Table 43 Queue Setup: Add/Edit

LABEL	DESCRIPTION
Active	Select to enable or disable this queue.
Name	Enter the descriptive name of this queue.
Interface	This shows the name of the ZyXEL Device's interface through which traffic in this queue passes.

Table 43 Queue Setup: Add/Edit

LABEL	DESCRIPTION
Priority	Select the priority level (from 1 to 7) of this queue. The larger the number, the higher the priority level. Traffic assigned to higher priority queues gets through faster while traffic in lower priority queues is dropped if the network is congested.
Weight	Select the weight (from 1 to 15) of this queue. If two queues have the same priority level, the ZyXEL Device divides the bandwidth across the queues according to their weights. Queues with larger weights get more bandwidth than queues with smaller weights.
Rate Limit	Specify the maximum transmission rate (in Kbps) allowed for traffic on this queue.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

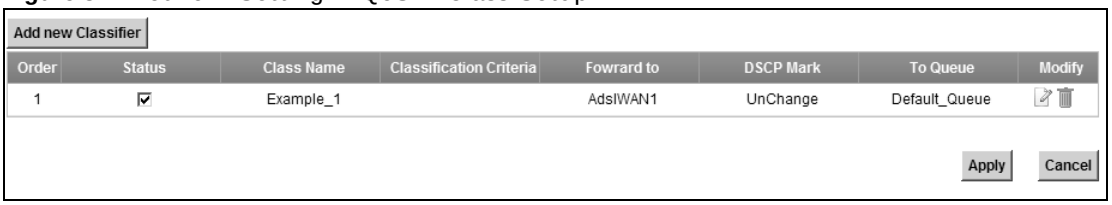
10.4 The Class Setup Screen

Use this screen to add, edit or delete QoS classifiers. A classifier groups traffic into data flows according to specific criteria such as the source address, destination address, source port number, destination port number or incoming interface. For example, you can configure a classifier to select traffic from the same protocol port (such as Telnet) to form a flow.

You can give different priorities to traffic that the ZyXEL Device forwards out through the WAN interface. Give high priority to voice and video to make them run more smoothly. Similarly, give low priority to many large file downloads so that they do not reduce the quality of other applications.

Click **Network Setting > QoS > Class Setup** to open the following screen.

Figure 81 Network Setting > QoS > Class Setup



The following table describes the labels in this screen.

Table 44 Network Setting > QoS > Class Setup

LABEL	DESCRIPTION
Add new Classifier	Click this to create a new classifier.
Order	This field displays the order number of the classifier.
Status	Select the check box to enable the classifier.
Class Name	This is the name of the classifier.
Classification Criteria	This shows criteria specified in this classifier, for example the interface from which traffic of this class should come and the source MAC address of traffic that matches this classifier.
Forward to	This is the interface through which traffic that matches this classifier is forwarded out.
DSCP Mark	This is the DSCP number added to traffic of this classifier.

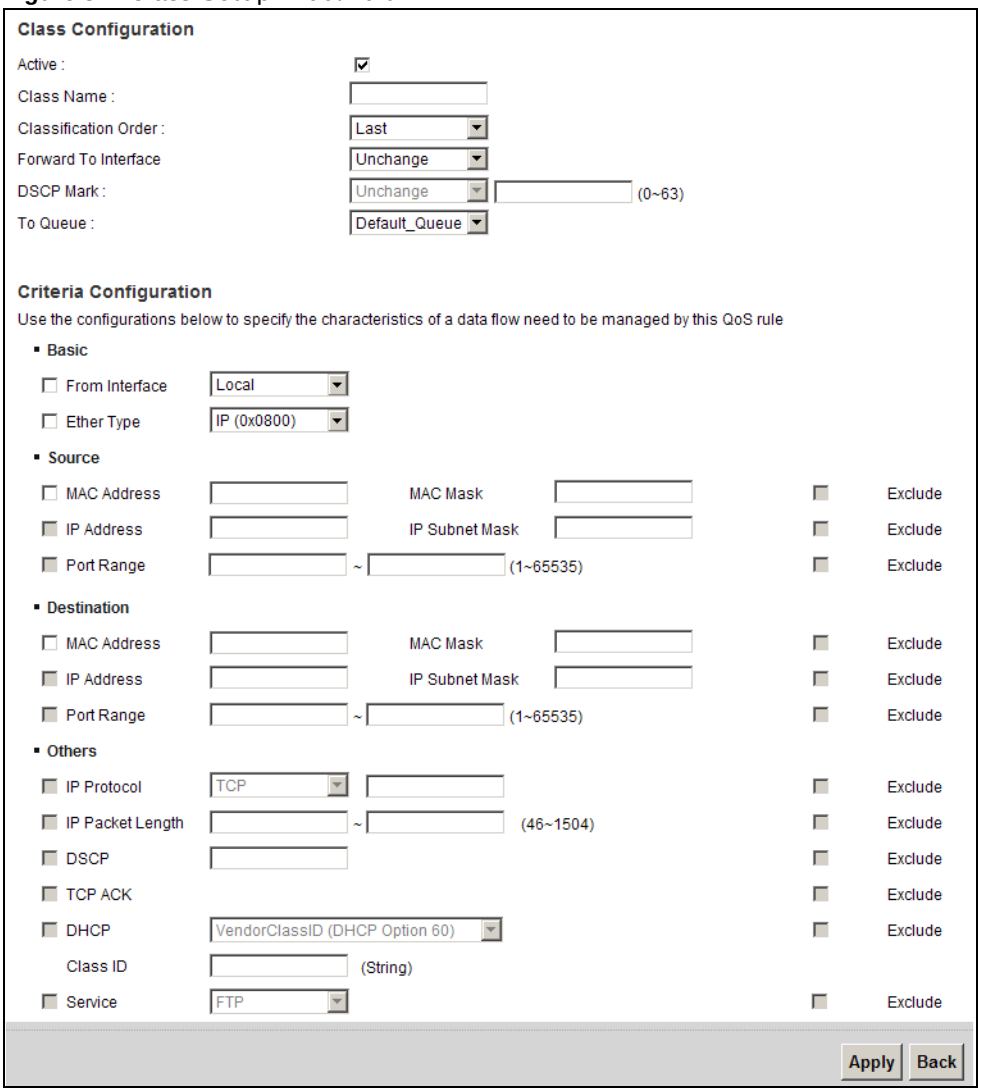
Table 44 Network Setting > QoS > Class Setup (continued)

LABEL	DESCRIPTION
To Queue	This is the name of the queue in which traffic of this classifier is put.
Modify	Click the **Edit** icon to edit the classifier. Click the **Delete** icon to delete an existing classifier. Note that subsequent rules move up by one when you take this action.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

10.4.1 Add/Edit QoS Class

Click **Add new Classifier** in the **Class Setup** screen or the **Edit** icon next to an existing classifier to configure it.

Figure 82 Class Setup: Add/Edit


Class Configuration
Active :
Class Name :
Classification Order : Last
Forward To Interface : Unchange
DSCP Mark : Unchange (0~63)
To Queue : Default_Queue
Criteria Configuration
Use the configurations below to specify the characteristics of a data flow need to be managed by this QoS rule
Basic
From Interface : Local
Ether Type : IP (0x0800)
Source
MAC Address MAC Mask Exclude
IP Address IP Subnet Mask Exclude
Port Range ~ (1~65535) Exclude
Destination
MAC Address MAC Mask Exclude
IP Address IP Subnet Mask Exclude
Port Range ~ (1~65535) Exclude
Others
IP Protocol : TCP Exclude
IP Packet Length ~ (46~1504) Exclude
DSCP Exclude
TCP ACK Exclude
DHCP : VendorClassID (DHCP Option 60) Exclude
Class ID (String)
Service : FTP Exclude
Apply
Back

The following table describes the labels in this screen.

Table 45 Class Setup: Add/Edit

LABEL	DESCRIPTION
Class Configuration	
Active	Select to enable this classifier.
Class Name	Enter a descriptive name of up to 32 printable English keyboard characters, including spaces.
Classification Order	Select an existing number for where you want to put this classifier to move the classifier to the number you selected after clicking **Apply**. Select **Last** to put this rule in the back of the classifier list.
Forward to Interface	Select a WAN interface through which traffic of this class will be forwarded out. If you select **Unchange**, the ZyXEL Device forward traffic of this class according to the default routing table.
DSCP Mark	This field is available only when you select the **Ether Type** check box in **Criteria Configuration-Basic** section. If you select **Mark**, enter a DSCP value with which the ZyXEL Device replaces the DSCP field in the packets. If you select **Unchange**, the ZyXEL Device keep the DSCP field in the packets.
To Queue	Select a queue that applies to this class. You should have configured a queue in the **Queue Setup** screen already.
Criteria Configuration Use the following fields to configure the criteria for traffic classification.	
Basic	
From Interface	Select whether the traffic class comes from the LAN or a wireless interface.
Ether Type	Select a predefined application to configure a class for the matched traffic. If you select **IP**, you also need to configure source or destination MAC address, IP address, DHCP options, DSCP value or the protocol type.
Source	
MAC Address	Select the check box and enter the source MAC address of the packet.
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
IP Address	Select the check box and enter the source IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the source subnet mask.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Destination	
MAC Address	Select the check box and enter the destination MAC address of the packet.

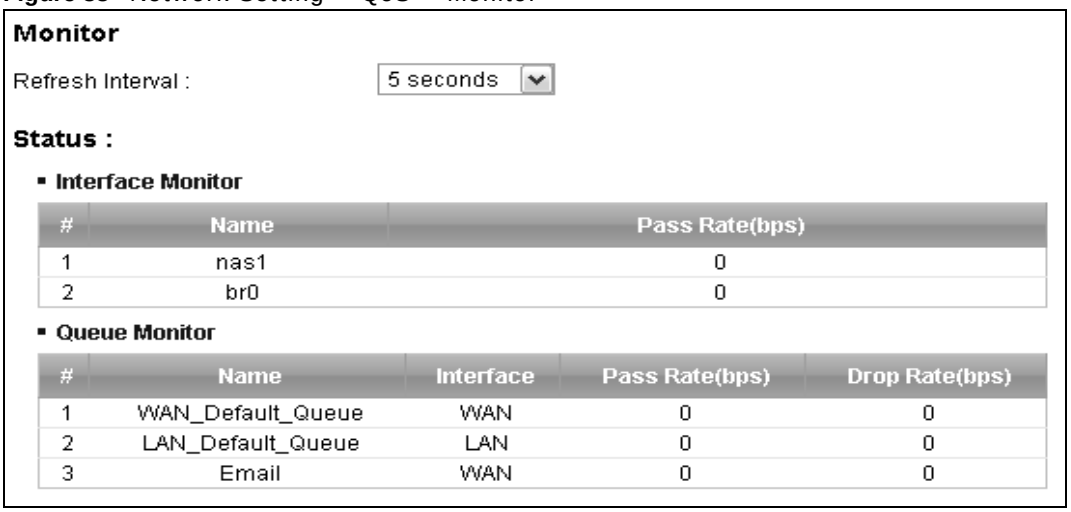
Table 45 Class Setup: Add/Edit (continued)

LABEL	DESCRIPTION
MAC Mask	Type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified source MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
IP Address	Select the check box and enter the destination IP address in dotted decimal notation. A blank source IP address means any source IP address.
IP Subnet Mask	Enter the destination subnet mask.
Port Range	If you select **TCP** or **UDP** in the **IP Protocol** field, select the check box and enter the port number(s) of the source.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Others	
IP Protocol	This field is available only when you select **IP** in the **Ether Type** field. Select this option and select the protocol (service type) from **TCP** or **UDP**. If you select **User defined**, enter the protocol (service type) number.
IP Packet Length	This field is available only when you select **IP** in the **Ether Type** field. Select this option and enter the minimum and maximum packet length (from 46 to 1504) in the fields provided.
DSCP	This field is available only when you select **IP** in the **Ether Type** field. Select this option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
TCP ACK	This field is available only when you select **IP** in the **Ether Type** field. If you select this option, the matched TCP packets must contain the ACK (Acknowledge) flag.
DHCP	This field is available only when you select **IP** in the **Ether Type** field, and **UDP** in the **IP Protocol** field. Select this option and select a DHCP option. If you select **Vendor Class ID (DHCP Option 60)**, enter the **Class ID** of the matched traffic, such as the type of the hardware or firmware. If you select **ClientID (DHCP Option 61)**, enter the **Type** of the matched traffic and **Client ID** of the DHCP client. If you select **User Class ID (DHCP Option 77)**, enter the **User Class Data**, which is a string that identifies the user's category or application type in the matched DHCP packets. If you select **VendorSpecificIntro (DHCP Option 125)**, enter the **Enterprise Number** of the software of the matched traffic and **Vendor Class Data** used by all the DHCP clients.
Service	Select the service classification of the traffic.
Exclude	Select this option to exclude the packets that match the specified criteria from this classifier.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

10.5 The QoS Monitor Screen

To view the ZyXEL Device's QoS packet statistics, click **Network Setting > QoS > Monitor**. The screen appears as shown.

Figure 83 Network Setting > QoS > Monitor



The following table describes the labels in this screen.

Table 46 Network Setting > QoS > Monitor

LABEL	DESCRIPTION
Monitor	
Refresh Interval	Select how often you want the ZyXEL Device to update this screen. Select **No Refresh** to stop refreshing statistics.
Status	
#	This is the index number of the entry.
Name	This shows the name of the WAN interface on the ZyXEL Device.
Pass Rate (bps)	This shows how many packets forwarded to this interface are transmitted successfully.
Queue Monitor	
#	This is the index number of the entry.
Name	This shows the name of the queue.
Interface	The type of connection that the traffic is going through
Pass Rate (bps)	This shows how many packets assigned to this queue are transmitted successfully.
Drop Rate (bps)	This shows how many packets assigned to this queue are dropped.

10.6 QoS Technical Reference

This section provides some technical background information about the topics covered in this chapter.

10.6.1 IP Precedence

Similar to IEEE 802.1p prioritization at layer-2, you can use IP precedence to prioritize packets in a layer-3 network. IP precedence uses three bits of the eight-bit ToS (Type of Service) field in the IP header. There are eight classes of services (ranging from zero to seven) in IP precedence. Zero is the lowest priority level and seven is the highest.

10.6.2 DiffServ

QoS is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

DiffServ (Differentiated Services) is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.

DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

DSCP (6 bits)	Unused (2 bits)

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different kinds of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

11

Network Address Translation (NAT)

11.1 Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

11.1.1 What You Can Do in this Chapter

- Use the **Port Forwarding** screen to configure forward incoming service requests to the server(s) on your local network (Section 11.2 on page 176).
- Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use (Section 11.3 on page 178).
- Use the **ALG** screen (Section 11.4 on page 179) to enable and disable the SIP (VoIP) ALG in the ZyXEL Device.

11.1.2 What You Need To Know

The following terms and concepts may help as you read this chapter.

Inside/Outside and Global/Local

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

NAT

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host.

Port Forwarding

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though NAT makes your whole inside network appear as a single computer to the outside world.

Finding Out More

See Section 11.5 on page 180 for advanced technical information on NAT.

11.2 The Port Forwarding Screen

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

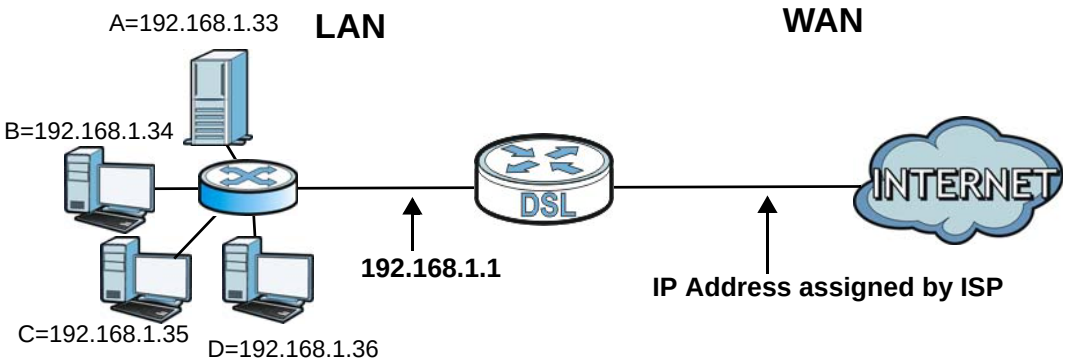
The most often used port numbers and services are shown in Appendix E on page 331. Please refer to RFC 1700 for further information about port numbers.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Configuring Servers Behind Port Forwarding (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 84 Multiple Servers Behind NAT Example

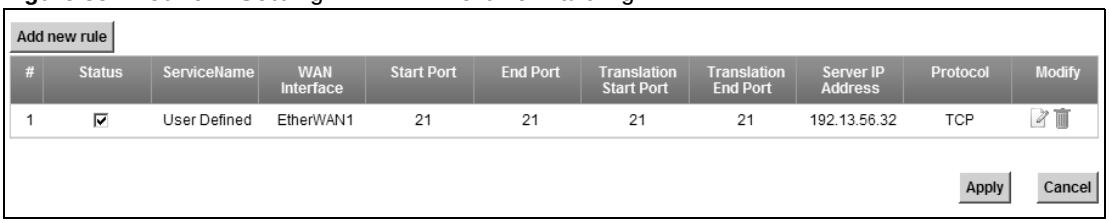


11.2.1 The Port Forwarding Screen

Click **Network Setting > NAT** to open the **Port Forwarding** screen.

See Appendix E on page 331 for port numbers commonly used for particular services.

Figure 85 Network Setting > NAT > Port Forwarding


Add new rule
Status ServiceName WAN Interface Start Port End Port Translation Start Port Translation End Port Server IP Address Protocol Modify
1 User Defined EtherWAN1 21 21 21 21 192.13.56.32 TCP
Apply
Cancel

The following table describes the fields in this screen.

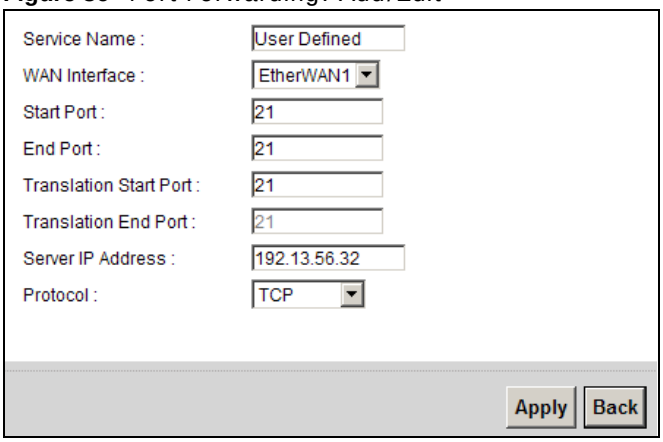
Table 47 Network Setting > NAT > Port Forwarding

LABEL	DESCRIPTION
Add new rule	Click this to add a new port forwarding rule.
#	This is the index number of the entry.
Status	This field indicates whether the rule is active or not. Clear the check box to disable the rule. Select the check box to enable it.
Service Name	This is the service's name. This shows **User Defined** if you manually added a service. You can change this by clicking the edit icon.
WAN Interface	This shows the WAN interface through which the service is forwarded.
Start Port	This is the first external port number that identifies a service.
End Port	This is the last external port number that identifies a service.
Translation Start Port	This is the first internal port number that identifies a service.
Translation End Port	This is the last internal port number that identifies a service.
Server IP Address	This is the server's IP address.
Protocol	This shows the IP protocol supported by this virtual server, whether it is **TCP**, **UDP**, or **TCP/UDP**.
Modify	Click the **Edit** icon to edit the port forwarding rule. Click the **Delete** icon to delete an existing port forwarding rule. Note that subsequent address mapping rules move up by one when you take this action.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

11.2.2 The Port Forwarding Edit Screen

This screen lets you create or edit a port forwarding rule. Click **Add new rule** in the **Port Forwarding** screen or the **Edit** icon next to an existing rule to open the following screen.

Figure 86 Port Forwarding: Add/Edit



The following table describes the labels in this screen.

Table 48 Port Forwarding: Add/Edit

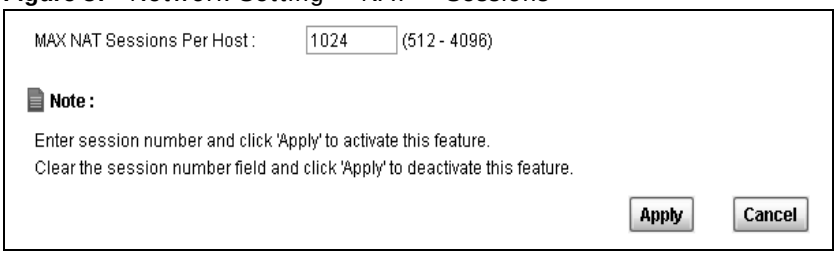
LABEL	DESCRIPTION
Service Name	Enter a name to identify this rule using keyboard characters (A-Z, a-z, 1-2 and so on).
WAN Interface	Select the WAN interface through which the service is forwarded. You must have already configured a WAN connection with NAT enabled.
Start Port	Enter the original destination port for the packets. To forward only one port, enter the port number again in the **External End Port** field. To forward a series of ports, enter the start port number here and the end port number in the **External End Port** field.
End Port	Enter the last port of the original destination port range. To forward only one port, enter the port number in the **External Start Port** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **External Start Port** field above.
Translation Start Port	This shows the port number to which you want the ZyXEL Device to translate the incoming port. For a range of ports, enter the first number of the range to which you want the incoming ports translated.
Translation End Port	This shows the last port of the translated port range.
Server IP Address	Enter the inside IP address of the virtual server here.
Protocol Type	Select the protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP/UDP**.
Apply	Click **Apply** to save your changes.
Back	Click **Back** to return to the previous screen without saving.

11.3 The Sessions Screen

Use the **Sessions** screen to limit the number of concurrent NAT sessions each client can use.

Click **Network Setting > NAT > Sessions** to display the following screen.

Figure 87 Network Setting > NAT > Sessions


MAX NAT Sessions Per Host :
1024
(512 - 4096)
Note :
Enter session number and click 'Apply' to activate this feature.
Clear the session number field and click 'Apply' to deactivate this feature.
Apply
Cancel

The following table describes the fields in this screen.

Table 49 Network Setting > NAT > Sessions

LABEL	DESCRIPTION
MAX NAT Sessions	Use this field to set a common limit to the number of concurrent NAT sessions each client computer can have. If only a few clients use peer to peer applications, you can raise this number to improve their performance. With heavy peer to peer application use, lower this number to ensure no single client uses too many of the available NAT sessions.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

11.4 The ALG Screen

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the ZyXEL Device registers with the SIP register server, the SIP ALG translates the ZyXEL Device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your ZyXEL Device is behind a SIP ALG.

Use this screen to enable and disable the SIP (VoIP) ALG in the ZyXEL Device. To access this screen, click **Network Setting > NAT > ALG**.

Figure 88 Network > NAT > ALG



The following table describes the fields in this screen.

Table 50 Network > NAT > ALG

LABEL	DESCRIPTION
ALG	Select enable to make sure SIP (VoIP) works correctly with port-forwarding and address-mapping rules.
Apply	Click this to save your changes.

11.5 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

11.5.1 NAT Definitions

Inside/outside denotes where a host is located relative to the ZyXEL Device, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 51 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

11.5.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

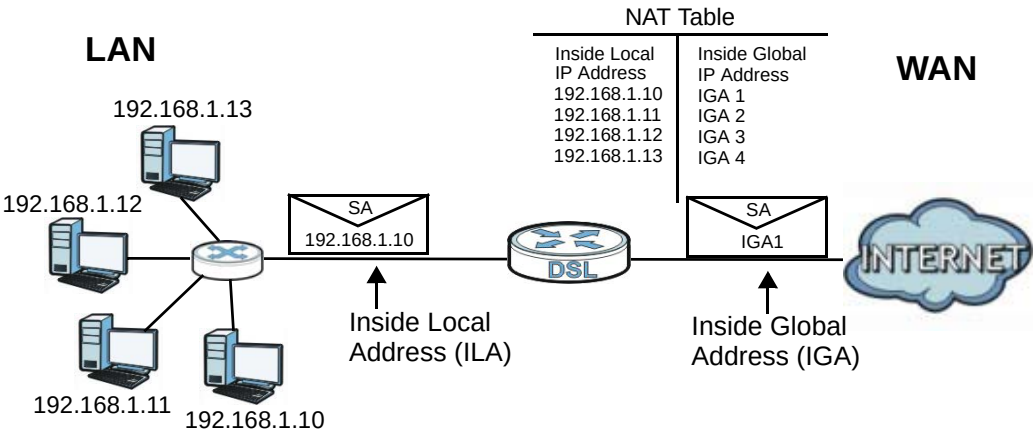
The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a Telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your ZyXEL Device filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

11.5.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global

Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The ZyXEL Device keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

Figure 89 How NAT Works



12

Dynamic DNS

12.1 Overview

This chapter discusses how to configure your ZyXEL Device to use Dynamic DNS.

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in applications such as NetMeeting and CU-SeeMe). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

12.1.1 What You Need To Know

DYNDNS Wildcard

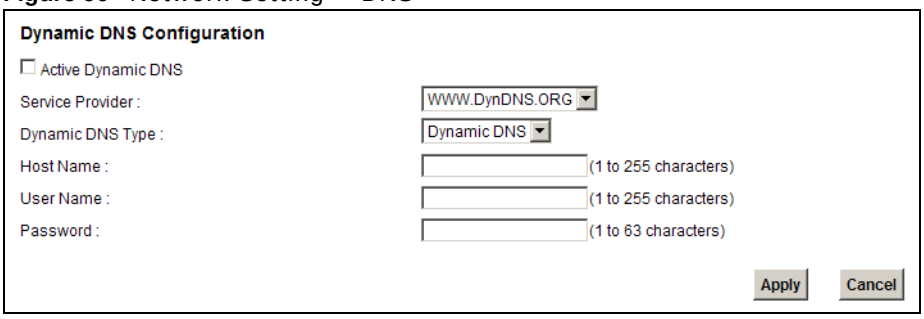
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

12.2 The Dynamic DNS Screen

Use the **Dynamic DNS** screen to enable DDNS and configure the DDNS settings on the ZyXEL Device. To change your ZyXEL Device's DDNS, click **Network Setting > Dynamic DNS**. The screen appears as shown.

Figure 90 Network Setting > DNS



The following table describes the fields in this screen.

Table 52 Network Setting > DNS

LABEL	DESCRIPTION
Dynamic DNS Configuration	
Active Dynamic DNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Type the domain name assigned to your ZyXEL Device by your Dynamic DNS provider. You can specify up to two host names in the field separated by a comma (",").
User Name	Type your user name.
Password	Type the password assigned to you.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

13

Firewall

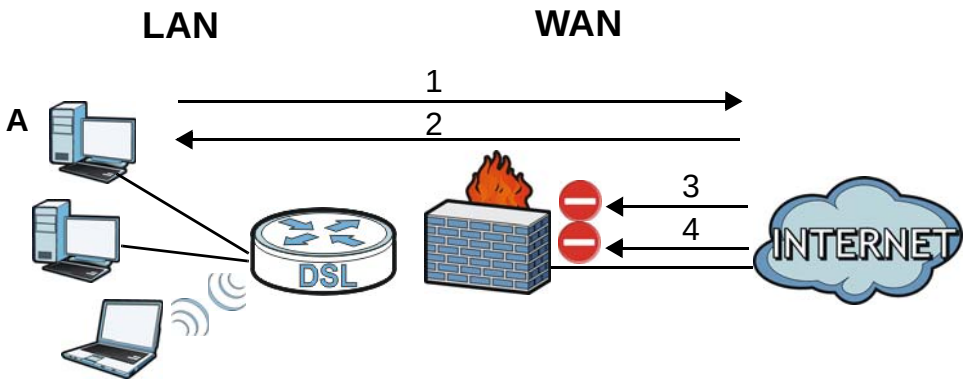
13.1 Overview

Use the ZyXEL Device firewall screens to enable and configure the firewall that protects your ZyXEL Device and network from attacks by hackers on the Internet and control access to it. By default the firewall:

- allows traffic that originates from your LAN and WLAN computers to go to all other networks.
- blocks traffic that originates on other networks from going to the LAN and WLAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN to the WAN (**1**). Return traffic for this session is also allowed (**2**). However other traffic initiated from the WAN is blocked (**3** and **4**).

Figure 91 Default Firewall Action



13.1.1 What You Can Do in this Chapter

- Use the **General** screen to enable or disable the ZyXEL Device's firewall (Section 13.2 on page 186).
- Use the **Services** screen to view the configured firewall rules and add, edit or remove a firewall rule (Section 13.3 on page 187).

13.1.2 What You Need to Know

Firewall

The ZyXEL Device's firewall feature physically separates the LAN/WLAN and the WAN and acts as a secure gateway for all data passing between the networks.

It is designed to protect against Denial of Service (DoS) attacks when activated. The ZyXEL Device's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The ZyXEL Device can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

The ZyXEL Device is installed between the LAN/WLAN and a broadband modem connecting to the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

ICMP

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

Finding Out More

See Section 13.4 on page 188 for advanced technical information on firewall.

13.2 The General Screen

Use this screen to enable or disable the ZyXEL Device's firewall. Click **Security > Firewall** to open the **General** screen.

Figure 92 Security > Firewall > General



The following table describes the labels in this screen.

Table 53 Security > Firewall > General

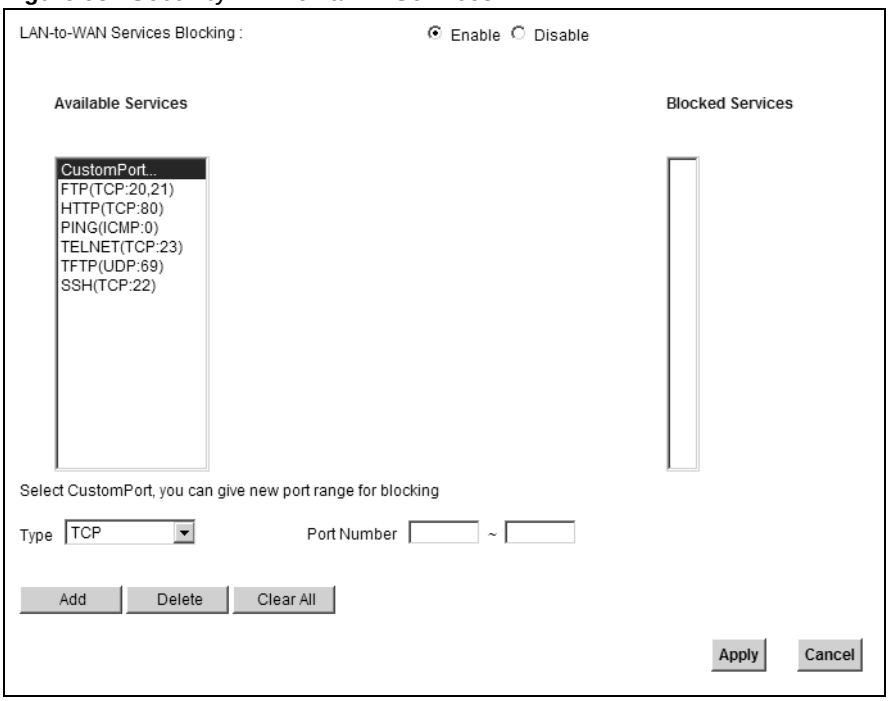
LABEL	DESCRIPTION
Firewall	Select **Enable** to activate the firewall. The ZyXEL Device performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

13.3 The Services Screen

Use this screen to enable service blocking and to maintain the list of services you want to block. To access this screen, click **Security > Firewall > Services**.

Note: These rules specify which computers on the LAN can access which computers or services on the WAN.

Figure 93 Security > Firewall > Services



Each field is described in the following table.

Table 54 Security > Firewall > Services

LABEL	DESCRIPTION
LAN-to-WAN Services Blocking	Select **Enable** to activate service blocking.
Available Services	This is a list of pre-defined services (destination ports) you may prohibit your LAN computers from using. Select the port you want to block, and click **Add** to add the port to the **Blocked Services** field. A custom port is a service that is not available in the pre-defined **Available Services** list. You must define it using the **Type** and **Port Number** fields. See Appendix E on page 331 for some examples of services.
Blocked Services	This is a list of services (ports) that are inaccessible to computers on your LAN when service blocking is effective. To remove a service from this list, select the service, and click **Delete**.
Type	Select **TCP**, **UDP** or **TCP and UDP**, based on which one the custom port uses.
Port Number	Enter the range of port numbers that defines the service. For example, suppose you want to define the Gnutella service. Select **TCP** type and enter a port range of **6345-6349**.
Add	Click this to add the selected service in **Available Services** to the **Blocked Services** list. Note that the service is blocked immediately after clicking this.

Table 54 Security > Firewall > Services (continued)

LABEL	DESCRIPTION
Delete	Select a service in the **Blocked Services**, and click this to remove the service from the list.
Clear All	Click this to remove all the services in the **Blocked Services** list.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

13.4 Firewall Technical Reference

This section provides some technical background information about the topics covered in this chapter.

13.4.1 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via web configurator.
2. Think about access control before you connect to the network in any way.
3. Limit who can access your ZyXEL Device.
4. Don't enable any local service (such as Telnet or FTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
5. For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
6. Keep the firewall in a secured (locked) room.

13.4.2 Security Considerations

Note: Incorrectly configuring the firewall may block valid access or introduce security risks to the ZyXEL Device and your protected network. Use caution when creating or deleting firewall rules and test your rules after you configure them.

Consider these security ramifications before creating a rule:

1. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
2. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
3. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.

4 Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of entering the information into the correct fields in the web configurator screens.

14

MAC Filter

14.1 Overview

This chapter discusses MAC address filtering.

You can configure the ZyXEL Device to permit access to clients based on their MAC addresses in the **MAC Filter** screen. This applies to wired and wireless connections.

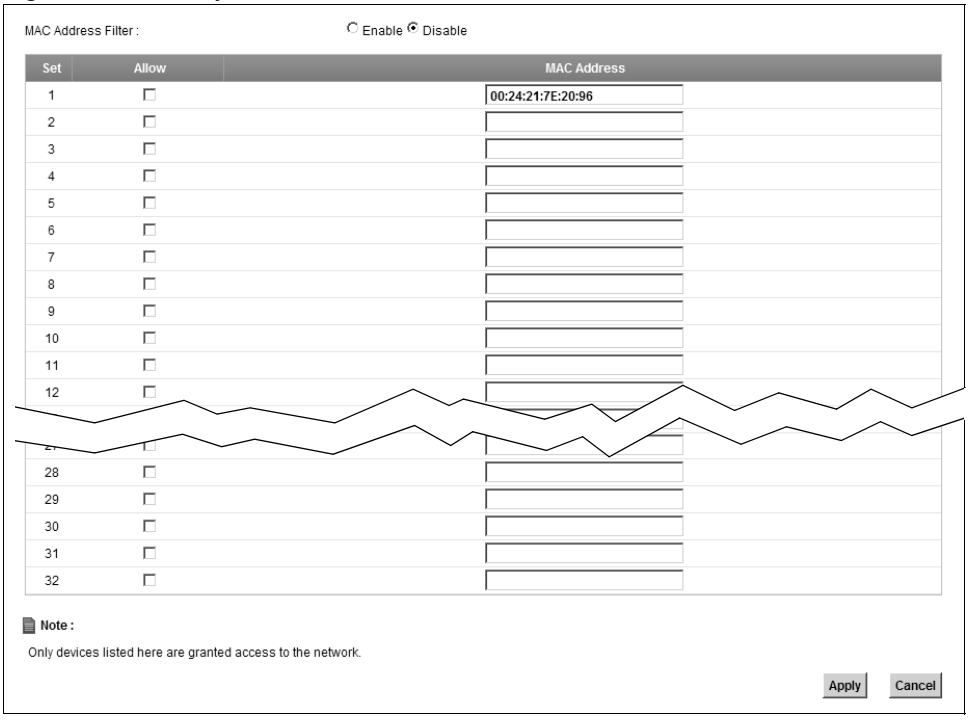
14.1.1 What You Need to Know

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

14.2 The MAC Filter Screen

Use the **MAC Filter** screen to allow wireless clients access to the ZyXEL Device. To change your ZyXEL Device's MAC filter settings, click **Security** > **MAC Filter**. The screen appears as shown.

Figure 94 Security > MAC Filter



The following table describes the labels in this menu.

Table 55 Security > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select **Enable** to activate MAC address filtering.
Set	This is the index number of the MAC address.
Allow	Select **Allow** to permit access to the ZyXEL Device. MAC addresses not listed will be denied access to the ZyXEL Device. If you clear this, the **MAC Address** field for this set clears.
MAC Address	Enter the MAC addresses of the wireless station that are allowed access to the ZyXEL Device in these address fields. Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

15

Certificates

15.1 Overview

The ZyXEL Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

15.1.1 What You Can Do in this Chapter

- Use the **Local Certificate** screens to view and import the ZyXEL Device's CA-signed certificates (Section 15.2 on page 196).
- Use the **Trusted CA** screens to save the certificates of trusted CAs to the ZyXEL Device. You can also export the certificates to a computer (Section 15.2.1 on page 197).

15.1.2 What You Need to Know

The following terms and concepts may help as you read this chapter.

Certification Authorities

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities.

Public and Private Keys

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

1. Tim wants to send a private message to Jenny. Tim generates a public-private key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

The ZyXEL Device uses certificates based on public-key cryptology to authenticate users attempting to establish a connection. The method used to secure the data that you send through an established connection depends on the type of connection. For example, a VPN tunnel might use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can then use the certification authority's public key to verify the certificates.

Certification Path

A certification path is the hierarchy of certification authority certificates that validate a certificate. The ZyXEL Device does not trust a certificate if any certificate on its path has expired or been revoked.

Certificate Directory Servers

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The ZyXEL Device can check a peer's certificate against a directory server's list of revoked certificates. The framework of servers, software, procedures and policies that handles keys is called PKI (public-key infrastructure).

Advantages of Certificates

Certificates offer the following benefits.

- The ZyXEL Device only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

Certificate File Formats

The certification authority certificate that you want to import has to be in one of these file formats:

- Binary X.509: This is an ITU-T recommendation that defines the formats for X.509 certificates.
- PEM (Base-64) encoded X.509: This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.
- Binary PKCS#7: This is a standard that defines the general syntax for data (including digital signatures) that may be encrypted. The ZyXEL Device currently allows the importation of a PKS#7 file that contains a single certificate.
- PEM (Base-64) encoded PKCS#7: This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

Note: Be careful not to convert a binary file to text during the transfer process. It is easy for this to occur since many programs use text files by default.

15.1.3 Verifying a Certificate

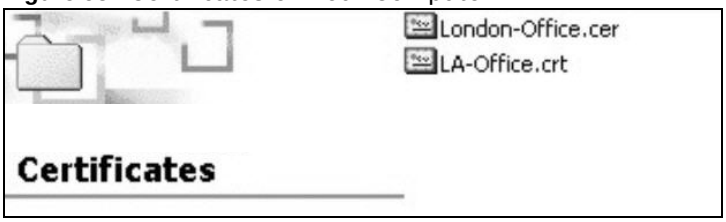
Before you import a trusted CA or trusted remote host certificate into the ZyXEL Device, you should verify that you have the actual certificate. This is especially true of trusted CA certificates since the ZyXEL Device also trusts any valid certificate signed by any of the imported trusted CA certificates.

You can use a certificate's fingerprint to verify it. A certificate's fingerprint is a message digest calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

1 Browse to where you have the certificate saved on your computer.

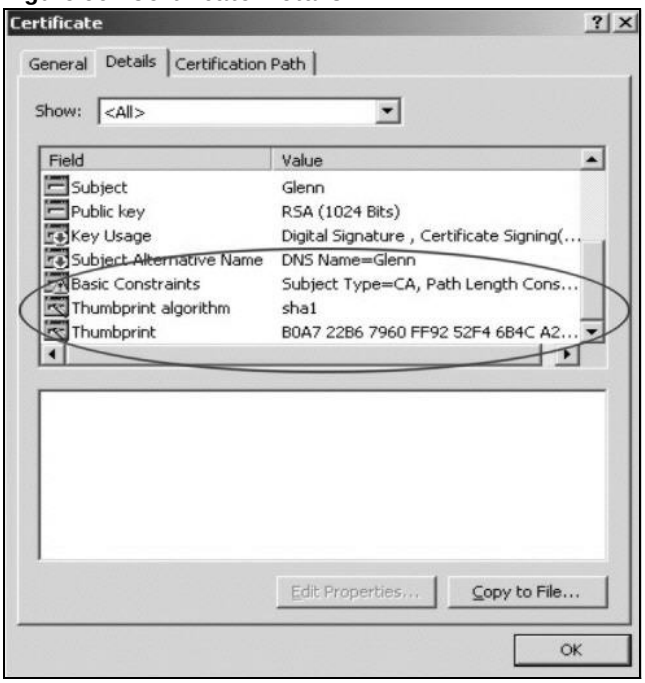
2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 95 Certificates on Your Computer



3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 96 Certificate Details



4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may very based on your situation. Possible examples would be over the telephone or through an HTTPS connection.

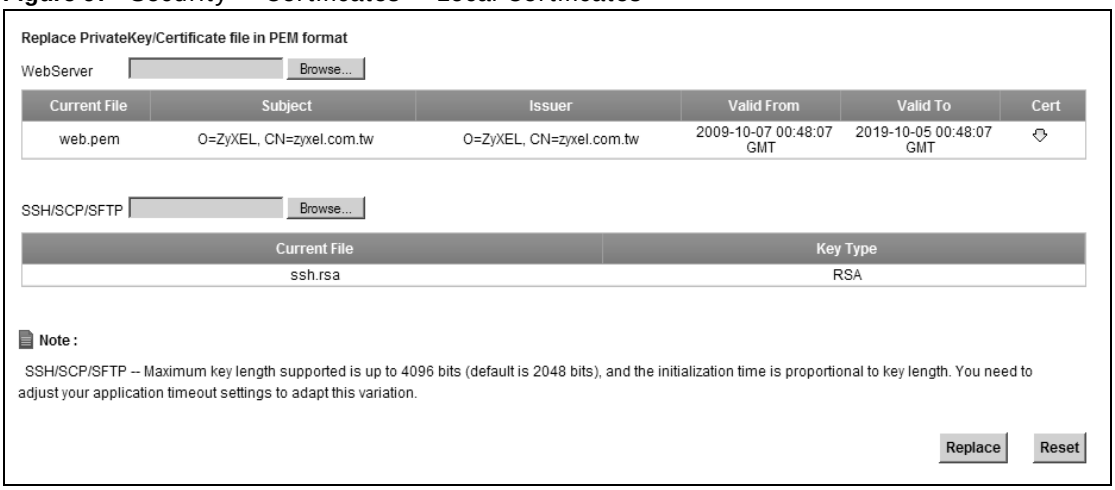
15.2 Local Certificates

Use this screen to view the ZyXEL Device's summary list of certificates and certification requests. You can import the following certificates to your ZyXEL Device:

- Web Server - This certificate secures HTTP connections.
- SSH/SCP/SFTP - This certificate secures remote connections.

Click **Security > Certificates** to open the **Local Certificates** screen.

Figure 97 Security > Certificates > Local Certificates



The following table describes the labels in this screen.

Table 56 Security > Certificates > Local Certificates

LABEL	DESCRIPTION
Web Server	Type in the location of the **Web Server** certificate file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Subject	This field displays identifying information about the certificate's owner, such as **CN** (Common Name), **OU** (Organizational Unit or department), **O** (Organization or company) and **C** (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Cert	Click this button and then **Save** in the **File Download** screen. The **Save As** screen opens, browse to the location that you want to use and click **Save**.
SSH/SCP/SFTP	Type in the location of the **SSH / SCP / SFTP** certificate file you want to upload in this field or click **Browse** to find it.

Table 56 Security > Certificates > Local Certificates (continued)

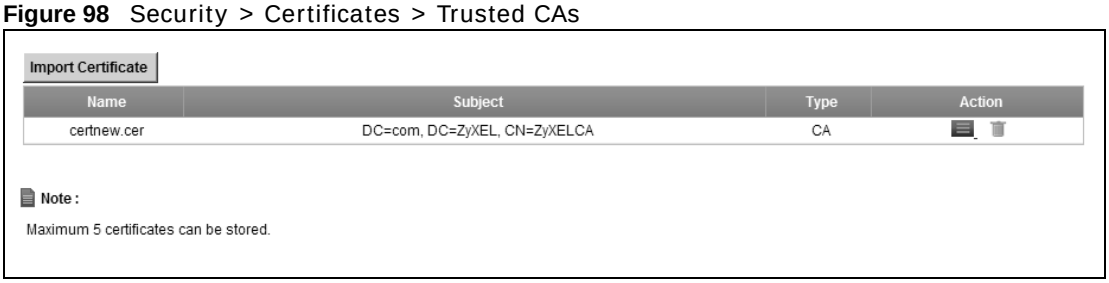
LABEL	DESCRIPTION
Browse	Click **Browse** to find the certificate file you want to upload.
Current File	This field displays the name used to identify this certificate. It is recommended that you give each certificate a unique name.
Key Type	This field applies to the **SSH / SCP / SFTP** certificate. This shows the file format of the current certificate.
Replace	Click this to replace the certificate(s) and save your changes back to the ZyXEL Device.
Reset	Click this to clear your settings.

15.2.1 Trusted CAs

Use this screen to view a summary list of certificates of the certification authorities that you have set the ZyXEL Device to accept as trusted. The ZyXEL Device accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Click **Security > Certificates > Trusted CAs** to open the **Trusted CAs** screen.

Figure 98 Security > Certificates > Trusted CAs



The following table describes the labels in this screen.

Table 57 Security > Certificates > Trusted CAs

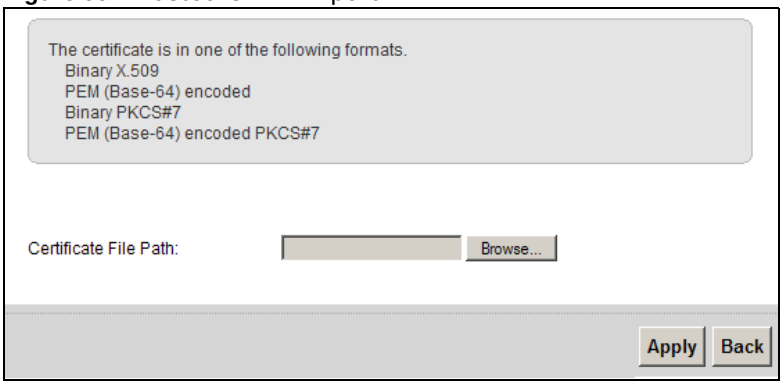
LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the ZyXEL Device.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Type	This field displays general information about the certificate. **ca** means that a Certification Authority signed the certificate.
Action	Click the **View** icon to open a screen with an in-depth list of information about the certificate (or certification request). Click the **Delete** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

15.2.2 Trusted CA Import

Click **Import Certificate** in the **Trusted CAs** screen to open the **Import Certificate** screen. You can save a trusted certification authority's certificate to the ZyXEL Device.

Note: You must remove any spaces from the certificate's filename before you can import the certificate.

Figure 99 Trusted CA > Import



The following table describes the labels in this screen.

Table 58 Security > Certificates > Trusted CA > Import

LABEL	DESCRIPTION
Certificate File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse	Click **Browse** to find the certificate file you want to upload.
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Back	Click **Back** to return to the previous screen.

15.2.3 View Certificate

Use this screen to view in-depth information about the certification authority's certificate, change the certificate's name and set whether or not you want the ZyXEL Device to check a certification authority's list of revoked certificates before trusting a certificate issued by the certification authority.

Click **Security** > **Certificates** > **Trusted CAs** to open the **Trusted CAs** screen. Click the **View** icon to open the **View Certificate** screen.

Figure 100 Trusted CA: View



The following table describes the labels in this screen.

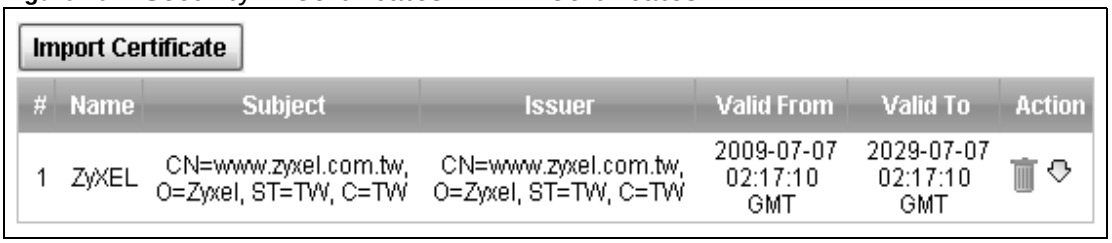
Table 59 Trusted CA: View

LABEL	DESCRIPTION
Certificate Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You may use any character (not including spaces).
Certificate Detail	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (via floppy disk for example).
Back	Click this to return to the previous screen.

15.3 VPN Certificates

To access this screen, click on Security > Certificates > VPN Certificates. Use this screen to...

Figure 101 Security > Certificates > VPN Certificates


Import Certificate
Name Subject Issuer Valid From Valid To Action
1 ZyXEL CN=www.zyxel.com.tw, O=Zyxel, ST=TW, C=TW CN=www.zyxel.com.tw, O=Zyxel, ST=TW, C=TW 2009-07-07 02:17:10 GMT 2029-07-07 02:17:10 GMT

The following table describes the labels in this screen.

Table 60 Security > Certificates > VPN Certificates

LABEL	DESCRIPTION
Import Certificate	Click this button to open a screen where you can save the certificate of a certification authority that you trust to the ZyXEL Device.
Name	This field displays the name used to identify this certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), OU (Organizational Unit or department), Organization (O), State (ST) and Country (C). It is recommended that each certificate have unique subject information.
Issuer	The certification authority
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a **Not Yet Valid!** message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an **Expiring!** or **Expired!** message if the certificate is about to expire or has already expired.
Action	Click the **Delete** icon to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.). Click on the **Download** icon to download a certificate to your computer.

15.3.1 Import Certificate

Click **Import Certificate** in the **VPN Certificates** screen to open the **Import Certificate** screen. You can save a trusted certification authority's certificate to the ZyXEL Device.

Figure 102 Security > Certificates > VPN Certificates



The following table describes the labels in this screen.

Table 61 VPN Certificates > Import

LABEL	DESCRIPTION
Name	Type a name for this certificate
Public Key	The value provided by a designated authority, which combined with a private key, can be used to encrypt messages. Write the key between **BEGIN CERTIFICATE** and **END CERTIFICATE**
Private Key	This is the key known only to the parties that exchange information. Write the key between **BEGIN CERTIFICATE** and **END CERTIFICATE**
Apply	Click **Apply** to save the certificate on the ZyXEL Device.
Back	Click **Back** to return to the previous screen.

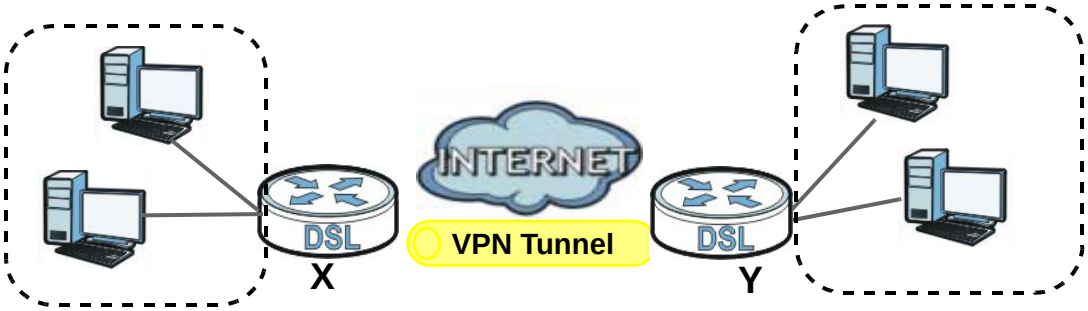
16 VPN

16.1 Overview

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer. The following figure is an example of an IPSec VPN tunnel.

Figure 103 VPN: Example



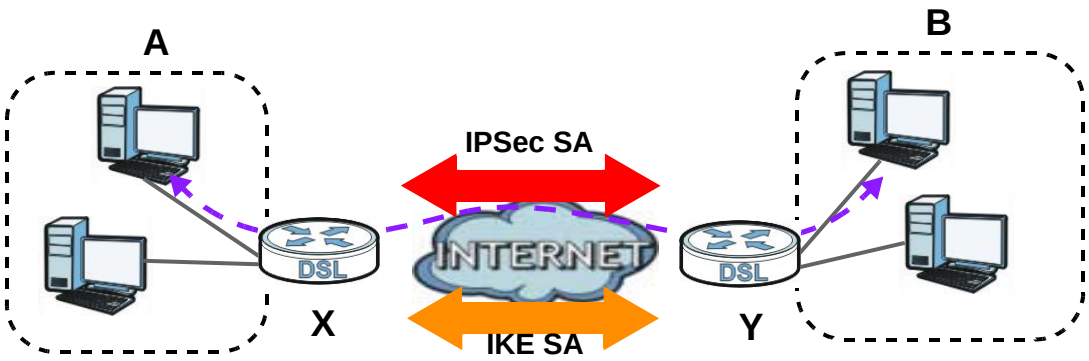
16.1.1 What You Can Do in the VPN Screens

- Use the **Setup** screen (Section 16.2 on page 205) to view the configured VPN policies and add, edit or remove a VPN policy.
- Use the **Monitor** screen (Section 16.5 on page 212) to display and manage the current active VPN connections.

16.1.2 What You Need to Know About IPSec VPN

A VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ZyXEL Device and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ZyXEL Device and remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the ZyXEL Device and remote IPSec router can send data between computers on the local network and remote network. The following figure illustrates this.

Figure 104 VPN: IKE SA and IPSec SA



In this example, a computer in network **A** is exchanging data with a computer in network **B**. Inside networks **A** and **B**, the data is transmitted the same way data is normally transmitted in the networks. Between routers **X** and **Y**, the data is protected by tunneling, encryption, authentication, and other security features of the IPSec SA. The IPSec SA is established securely using the IKE SA that routers **X** and **Y** established first.

My IP Address

My IP Address is the WAN IP address of the ZyXEL Device. The ZyXEL Device has to rebuild the VPN tunnel if **My IP Address** changes after setup.

The following applies if this field is configured as **0.0.0.0**:

- The ZyXEL Device uses the current ZyXEL Device WAN IP address (static or dynamic) to set up the VPN tunnel.

Secure Gateway Address

Secure Gateway Address is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static WAN IP address, enter it in the **Secure Gateway Address** field. You may alternatively enter the remote secure gateway's domain name (if it has one) in the **Secure Gateway Address** field.

You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The ZyXEL Device has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

Dynamic Secure Gateway Address

If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network (see Section 16.6.11 on page 219 for configuration examples).

The Secure Gateway IP Address may be configured as **0.0.0.0** only when using **IKE** key management and not **Manual** key management.

Finding Out More

See Section 16.6 on page 212 for advanced technical information on IPSec VPN.

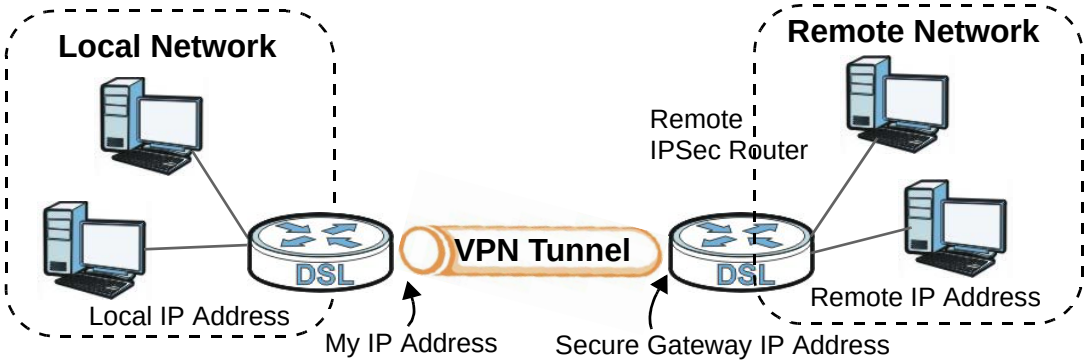
16.1.3 Before You Begin

If a VPN tunnel uses Telnet, FTP, WWW, then you should configure remote management (**Remote MGMT**) to allow access for that service.

16.2 VPN Setup Screen

The following figure helps explain the main fields in the web configurator.

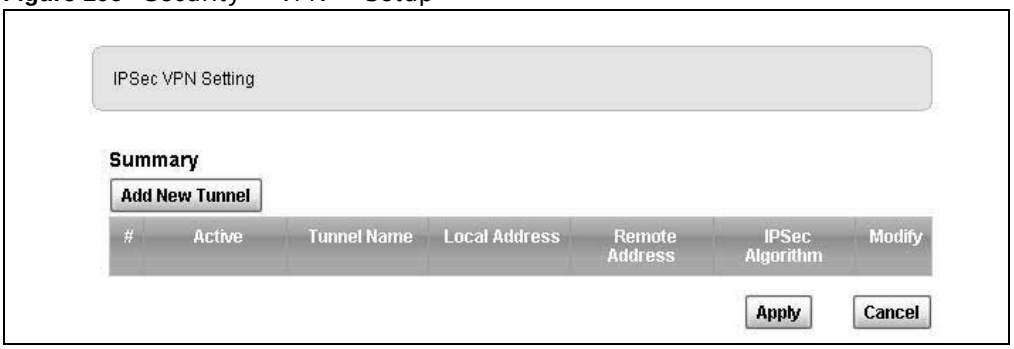
Figure 105 IPSec Summary Fields



Local and remote IP addresses must be static.

Click **Security** > **VPN** to open the **VPN Setup** screen. This is a menu of your IPSec rules (tunnels). The IPSec summary menu is read-only. Edit a VPN by selecting an index number and then configuring its associated submenus.

Figure 106 Security > VPN > Setup



The following table describes the fields in this screen.

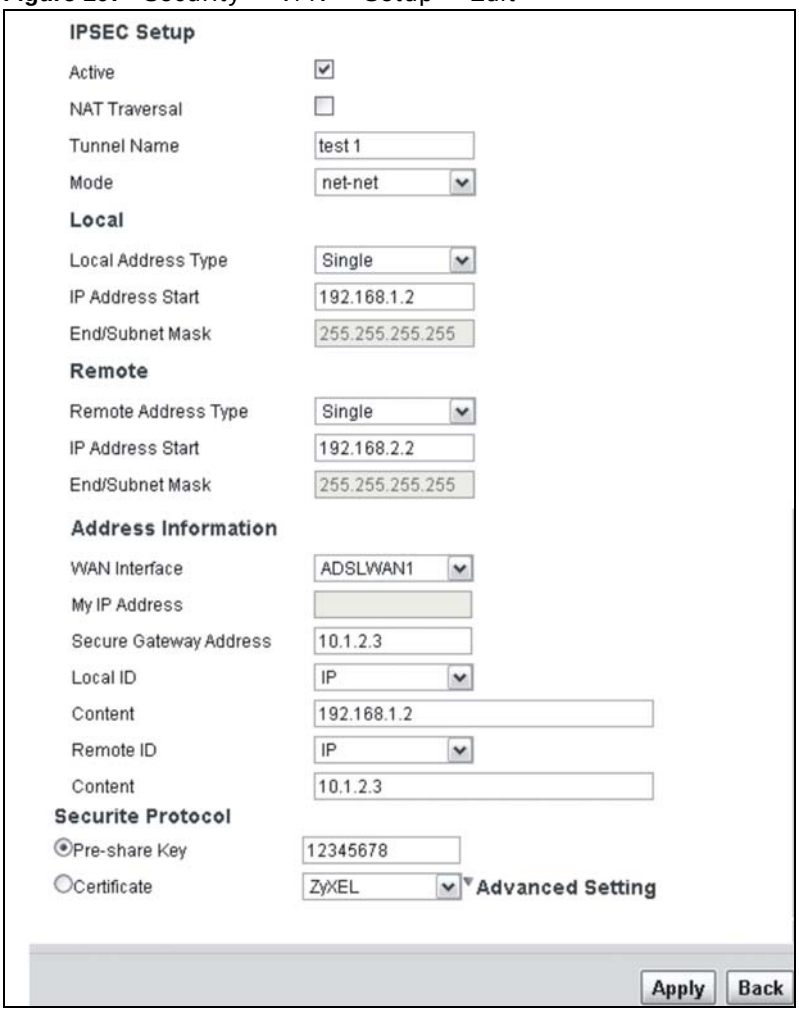
Table 62 Security > VPN > Setup

LABEL	DESCRIPTION
Add New Tunnel	Click this button to set up VPN policies for a new tunnel
#	This is the VPN policy index number. Click a number to edit VPN policies.
Active	This field displays whether the VPN policy is active or not. A **Yes** signifies that this VPN policy is active. **No** signifies that this VPN policy is not active.
Tunnel Name	This field displays the identification name for this VPN policy.
Local Address	This field will display the IP address used by the ZyXEL Device.
Remote Address	This field will display the Secure Gateway Address of the IPSec router with which you're making the VPN connection
IPSec Algorithm	This field displays the encryption algorithm used for an SA. Both **AH** and **ESP** increase ZyXEL Device processing requirements and communications latency (delay).
Modify	Click the **Edit** icon to go to the screen where you can edit the VPN configuration. Click the **Remove** icon to remove an existing VPN configuration.
Apply	Click this to save your changes and apply them to the ZyXEL Device.
Cancel	Click this return your settings to their last saved values.

16.3 The VPN Edit Screen

Click on **Add New Tunnel** in the **VPN Setup** screen or click on the **Edit** icon to edit VPN policies. Both commands share the same screen.

Figure 107 Security > VPN > Setup > Edit



The following table describes the fields in this screen.

Table 63 Security > VPN > Setup > Edit

LABEL	DESCRIPTION
IPSec Setup	
Active	Select this check box to activate this VPN policy. This option determines whether a VPN rule is applied before a packet leaves the firewall.
NAT Traversal	Select this check box if you want to set up a VPN tunnel when there are NAT routers between the ZyXEL Device and remote IPSec router. The remote IPSec router must also enable NAT traversal, and the NAT routers have to forward UDP port 4500 packets to the remote IPSec router behind the NAT router.
Tunnel Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the ZyXEL Device drops trailing spaces.
Mode	Select **net-net** or **Roadwarrior** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.

Table 63 Security > VPN > Setup > Edit

LABEL	DESCRIPTION
Local	Specify the IP addresses of the devices behind the ZyXEL Device that can use the VPN tunnel. The local IP addresses must correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Local Address Type	Use the drop-down menu to choose **Single**, or **Subnet**. Select **Single** for a single IP address. Select **Subnet** to specify IP addresses based on the subnet mask.
IP Address Start	When the **Local Address Type** field is configured to **Single**, enter a (static) IP address on the LAN behind your ZyXEL Device. When the **Local Address Type** field is configured to **Subnet**, enter an IP address on the LAN behind your ZyXEL Device.
End / Subnet Mask	When the **Local Address Type** field is configured to **Single**, this field is N/A. When the **Local Address Type** field is configured to **Subnet**, enter the subnet of the LAN behind your ZyXEL Device.
Remote	Specify the IP addresses of the devices behind the remote IPSec router that can use the VPN tunnel. The remote IP addresses must correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address Type	Use the drop-down menu to choose **Single**, or **Subnet**. Select **Single** for a single IP address. Select **Subnet** to specify IP addresses based on the subnet mask.
IP Address Start	When the **Remote Address Type** field is configured to **Single**, enter a (static) IP address on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter an IP Address on the LAN behind the IPSec router.
End / Subnet Mask	When the **Remote Address Type** field is configured to **Single**, this field is N/A. When the **Remote Address Type** field is configured to **Subnet**, enter the subnet of the LAN behind the IPSec router.
Address Information	
WAN Interface	The interface used to connect to the internet
My IP Address	My IP Address only shows the IP of the selected interface. There is no need to modify this information.
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection. If you are not sure of this information you can leave it blank, but do not use 0.0.0.0.
Local ID	Select **IP** to identify this ZyXEL Device by its IP address. Select **DNS** to identify this ZyXEL Device by a domain name. Select **E-mail** to identify this ZyXEL Device by an e-mail address.

Table 63 Security > VPN > Setup > Edit

LABEL	DESCRIPTION
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The ZyXEL Device automatically uses the IP address in the **My IP Address** field (refer to the **My IP Address** field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this ZyXEL Device in the local **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.
Remote ID	Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Content	The configuration of the peer content depends on the peer ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the ZyXEL Device will use the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description). For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations: • When there is a NAT router between the two IPSec routers. • When you want the ZyXEL Device to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.
Security Protocol	
Pre-Shared Key	Click the button to use a pre-shared key for authentication, and type in your pre-shared key. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", “0x” denotes that the key is hexadecimal and “0123456789ABCDEF” is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a “PYLD_MALFORMED” (payload malformed) packet if the same pre-shared key is not used on both ends.
Certificate	Click the button to use a certificate for authentication. Select the certificate you want to use from the list. You can create, import and configure certificates in the **Security > Certificates** screens.

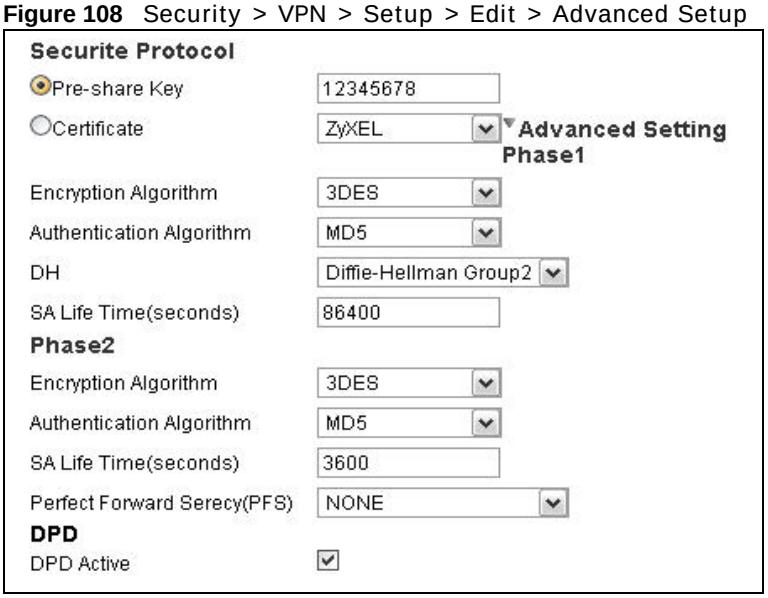
Table 63 Security > VPN > Setup > Edit

LABEL	DESCRIPTION
Advanced Setup	Click **Advanced Setup** to configure more detailed settings of your IKE key management.
Apply	Click **Apply** to save your changes back to the ZyXEL Device.
Back	Click **Back** to return to the previous screen.

16.4 Configuring Advanced Settings

Click **Advanced Setup** in the **VPN Setup-Edit** screen to open this screen.

Figure 108 Security > VPN > Setup > Edit > Advanced Setup



The following table describes the fields in this screen.

Table 64 Security > VPN > Setup > Edit > Advanced Setup

LABEL	DESCRIPTION
Advanced Setup	
Phase 1	
Encryption Algorithm	Select **3DES**, **AES128** or **AES256** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit key and a 256-bit key. **AES** is faster than **3DES**.

Table 64 Security > VPN > Setup > Edit > Advanced Setup (continued)

LABEL	DESCRIPTION
Authentication Algorithm	Select **MD5**, **SHA1**, **SHA2-256** or **SHA2-512** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) and **SHA2** are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for more security. **SHA2-256** or **SHA2-512** are part of the SHA2 set of cryptographic functions and they are considered even more secure than **MD5** and **SHA1**.
DH	You must choose a key group for phase 1 setup. **DH2** refers to Diffie-Hellman Group 2, a 1024-bit random number. **DH5** refers to Diffie-Hellman Group5, a 1536-bit random number, and **DH14** refers to Diffie-Hellman Group 14, providing 2048 bits of key strength.
SA Life Time (Seconds)	Define the length of time before an IPSec SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Phase 2	
Encryption Algorithm	Select **3DES, AES-128** or **AES-256** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a **128**-bit key and a **256**-bit key. **AES** is faster than **3DES**.
Authentication Algorithm	Select **MD5**, **SHA1**, **SHA2-256** or **SHA2-512** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) and **SHA2** are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for more security. **SHA2-256** or **SHA2-512** are part of the SHA2 set of cryptographic functions and they are considered even more secure than **MD5** and **SHA1**.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**NONE**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Choose **DH2**, **DH5** or **DH14** from the drop-down list box to enable PFS. **DH2** refers to Diffie-Hellman Group 2, a 1024-bit random number. **DH5** refers to Diffie-Hellman Group5, a 1536-bit random number, and **DH14** refers to Diffie-Hellman Group 14, providing 2048 bits of key strength.
DPD Active	Select DPD (Dead Peer Protection) if you want the ZyXEL Device to make sure the remote IPSec router is there before it transmits data. The remote IPSec router must support DPD. If there has been no traffic for at least 15 seconds, the ZyXEL Device sends a message to the remote IPSec router. If the remote IPSec router responds, the ZyXEL Device transmits the data. If the remote IPSec router does not respond, the ZyXEL Device shuts down the SA.
Apply	Click **Apply** to save your changes back to the ZyXEL Device and return to the **VPN** screen.
Back	Click **Back** to return to the previous screen.

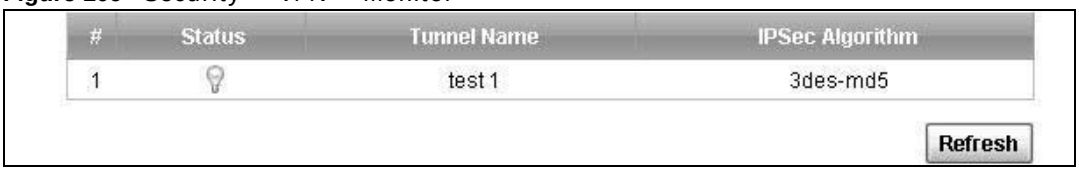
16.5 Viewing SA Monitor

Click **Security** > **VPN** > **Monitor** to open the screen as shown. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only. The following table describes the fields in this tab.

When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See Section 16.6.6 on page 217 on keeping alive to have the ZyXEL Device renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

Figure 109 Security > VPN > Monitor



The following table describes the fields in this screen.

Table 65 Security > VPN > Monitor

LABEL	DESCRIPTION
No	This is the security association index number.
Status	Displays whether the security association is active or not
Tunnel Name	This is the name of the new tunnel.
IPSec Algorithm	This field displays the encryption algorithm, and authentication algorithm used in each VPN tunnel.
Disconnect	Select one of the security associations, and then click **Disconnect** to stop that security association.
Refresh	Click **Refresh** to display the current active VPN connection(s).

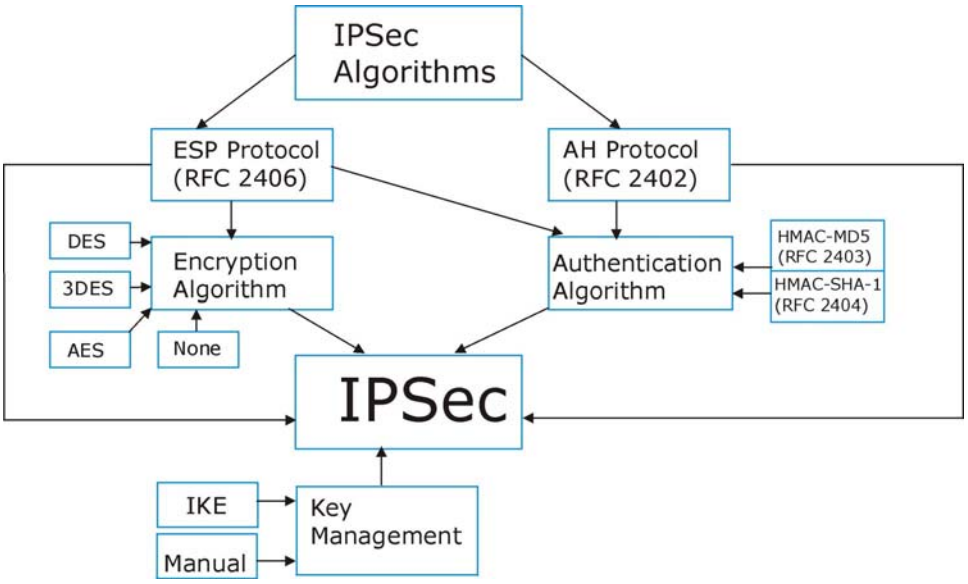
16.6 IPSec VPN Technical Reference

This section provides some technical background information about the topics covered in this chapter.

16.6.1 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 110 IPSec Architecture



IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols.

Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

16.6.2 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the ZyXEL Device.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT.

Table 66 VPN and NAT

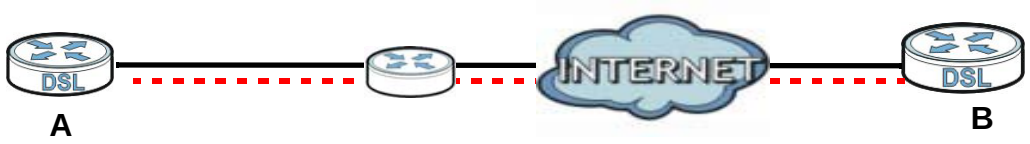
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

16.6.3 VPN, NAT, and NAT Traversal

NAT is incompatible with the AH protocol in both transport and tunnel mode. An IPSec VPN using the AH protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet, but a NAT device between the IPSec endpoints rewrites the source or destination address. As a result, the VPN device at the receiving end finds a mismatch between the hash value and the data and assumes that the data has been maliciously altered.

NAT is not normally compatible with ESP in transport mode either, but the ZyXEL Device's **NAT Traversal** feature provides a way to handle this. NAT traversal allows you to set up an IKE SA when there are NAT routers between the two IPSec routers.

Figure 111 NAT Router Between IPSec Routers



Normally you cannot set up an IKE SA with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. In Figure 111 on page 214, when IPSec router **A** tries to establish an IKE SA, IPSec router **B** checks the UDP port 500 header, and IPSec routers **A** and **B** build the IKE SA.

For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.

- Set the NAT router to forward UDP port 500 to IPSec router **A**.

Finally, NAT is compatible with ESP in tunnel mode because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device. The compatibility of AH and ESP with NAT in tunnel and transport modes is summarized in the following table.

Table 67 VPN and NAT

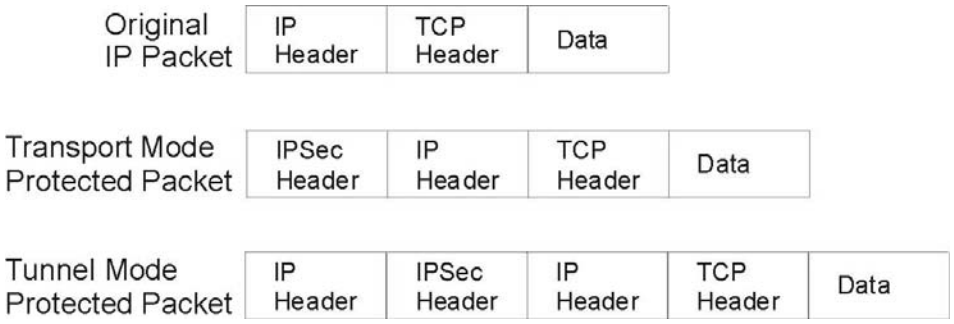
SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	Y*
ESP	Tunnel	Y

Y* - This is supported in the ZyXEL Device if you enable NAT traversal.

16.6.4 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

Figure 112 Transport and Tunnel Mode IPSec Encapsulation



Tunnel Mode

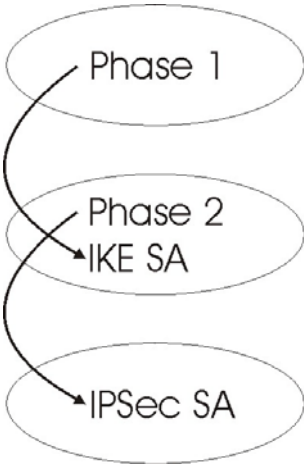
Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

16.6.5 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 113 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see Appendix D on page 311. Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The ZyXEL Device automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The ZyXEL Device also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

16.6.6 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

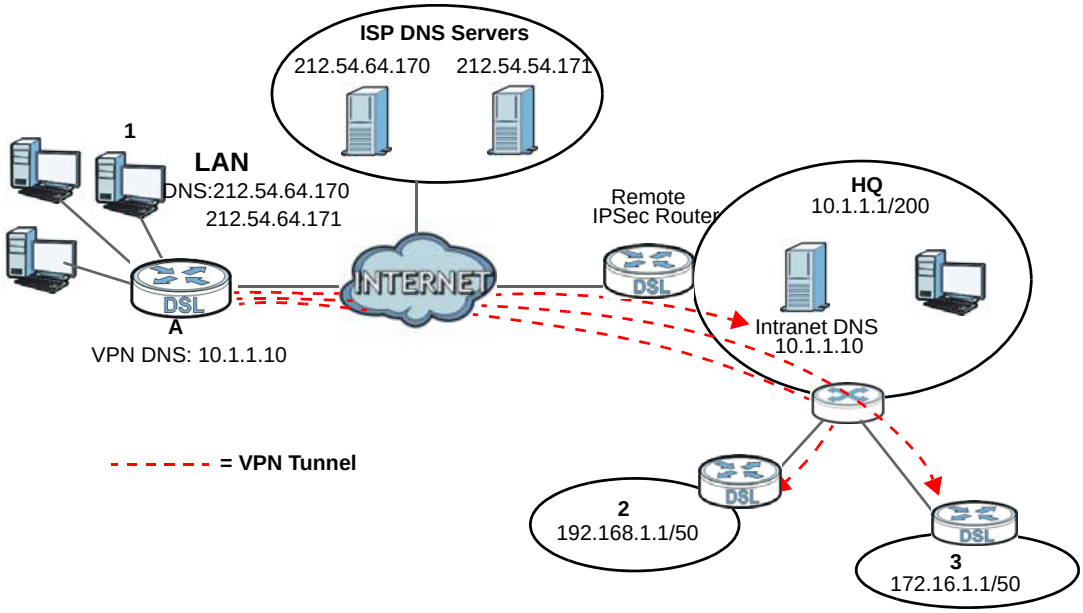
- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).

16.6.7 Remote DNS Server

In cases where you want to use domain names to access Intranet servers on a remote network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote network

The following figure depicts an example where three VPN tunnels are created from ZyXEL Device A; one to branch office 2, one to branch office 3 and another to headquarters. In order to access computers that use private domain names on the headquarters (HQ) network, the ZyXEL Device at branch office 1 uses the Intranet DNS server in headquarters. The DNS server feature for VPN does not work with Windows 2000 or Windows XP.

Figure 114 VPN Host using Intranet DNS Server Example



If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote network.

16.6.8 ID Type and Content

With aggressive negotiation mode (seeSection 16.6.6 on page 217), the ZyXEL Device identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the ZyXEL Device to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the ZyXEL Device from IPSec routers with dynamic IP addresses (seeSection 16.6.11 on page 219 for a telecommuter configuration example).

Regardless of the ID type and content configuration, the ZyXEL Device does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (seeSection 16.6.6 on page 217), the ID type and content are encrypted to provide identity protection. In this case the ZyXEL Device can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The ZyXEL Device can distinguish up to 12 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (seeSection 16.4 on page 210). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 68 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer or leave the field blank to have the ZyXEL Device automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this ZyXEL Device.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this ZyXEL Device.
	The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.

Table 69 Peer ID Type and Content Fields

PEER ID TYPE=	CONTENT=
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the ZyXEL Device automatically use the address in the **Secure Gateway Address** field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
	The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Address** field below.

16.6.8.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two ZyXEL Devices in this example can complete negotiation and establish a VPN tunnel.

Table 70 Matching ID Type and Content Configuration Example

ZYXEL DEVICE A	ZYXEL DEVICE B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two ZyXEL Devices in this example cannot complete their negotiation because ZyXEL Device B's **Local ID type** is **IP**, but ZyXEL Device A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 71 Mismatching ID Type and Content Configuration Example

ZYXEL DEVICE A	ZYXEL DEVICE B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

16.6.9 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see Section 16.6.5 on page 216 for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

16.6.10 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

16.6.11 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single ZyXEL Device at headquarters. The telecommuters use IPSec routers with dynamic WAN IP addresses. The ZyXEL Device at headquarters has a static public IP address.

16.6.11.1 Telecommuters Sharing One VPN Rule Example

See the following figure and table for an example configuration that allows multiple telecommuters (**A**, **B** and **C** in the figure) to use one VPN rule to simultaneously access a ZyXEL Device at headquarters (**HQ** in the figure). The telecommuters do not have domain names mapped to the

WAN IP addresses of their IPSec routers. The telecommuters must all use the same IPSec parameters but the local IP addresses (or ranges of addresses) should not overlap.

Figure 115 Telecommuters Sharing One VPN Rule Example

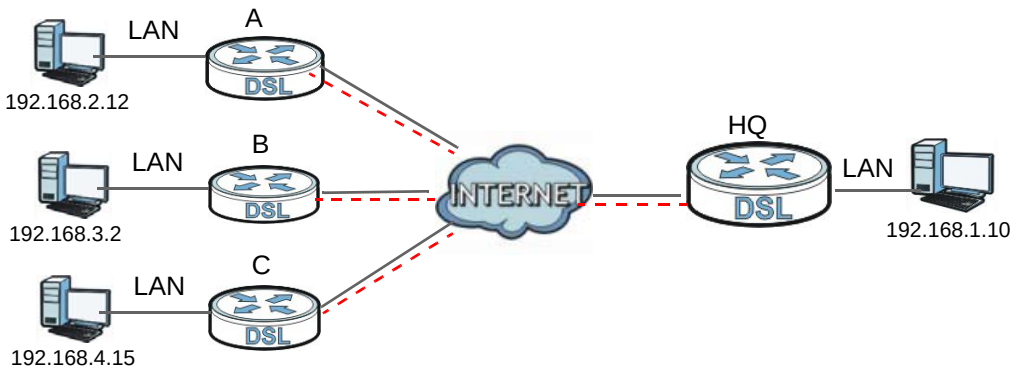


Table 72 Telecommuters Sharing One VPN Rule Example

FIELDS	TELECOMMUTERS	HEADQUARTERS
My IP Address:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Secure Gateway IP Address:	Public static IP address	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.
Local IP Address:	Telecommuter A: 192.168.2.12 Telecommuter B: 192.168.3.2 Telecommuter C: 192.168.4.15	192.168.1.10
Remote IP Address:	192.168.1.10	0.0.0.0 (N/A)

16.6.11.2 Telecommuters Using Unique VPN Rules Example

In this example the telecommuters (**A**, **B** and **C** in the figure) use IPSec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see Section 16.6.6 on page 217), the ZyXEL Device can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a ZyXEL Device at headquarters. They can use different IPSec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the ZyXEL Device at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters' IPSec routers should not overlap.

See the following table and figure for an example where three telecommuters each use a different VPN rule for a VPN connection with a ZyXEL Device located at headquarters. The ZyXEL Device at headquarters (**HQ** in the figure) identifies each incoming SA by its ID type and content and uses the appropriate VPN rule to establish the VPN connection.

The ZyXEL Device at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

Figure 116 Telecommuters Using Unique VPN Rules Example

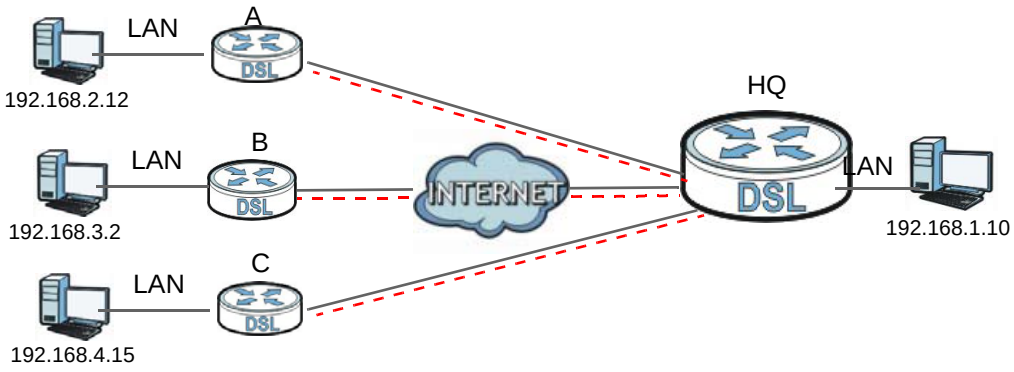


Table 73 Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
All Telecommuter Rules:	All Headquarters Rules:
0.0.0.0	My IP Address: bigcompanyhq.com
Secure Gateway Address: bigcompanyhq.com	Local IP Address: 192.168.1.10
Remote IP Address: 192.168.1.10	Local ID Type: E-mail
Peer ID Type: E-mail	Local ID Content: bob@bigcompanyhq.com
Peer ID Content: bob@bigcompanyhq.com	
Telecommuter A (telecommutera.dydns.org)	Headquarters ZyXEL Device Rule 1:
Local ID Type: IP	Peer ID Type: IP
Local ID Content: 192.168.2.12	Peer ID Content: 192.168.2.12
Local IP Address: 192.168.2.12	Secure Gateway Address: telecommuter1.com
	Remote Address 192.168.2.12
Telecommuter B (telecommuterb.dydns.org)	Headquarters ZyXEL Device Rule 2:
Local ID Type: DNS	Peer ID Type: DNS
Local ID Content: telecommuterb.com	Peer ID Content: telecommuterb.com
Local IP Address: 192.168.3.2	Secure Gateway Address: telecommuterb.com
	Remote Address 192.168.3.2
Telecommuter C (telecommuterc.dydns.org)	Headquarters ZyXEL Device Rule 3:
Local ID Type: E-mail	Peer ID Type: E-mail
Local ID Content: myVPN@myplace.com	Peer ID Content: myVPN@myplace.com
Local IP Address: 192.168.4.15	Secure Gateway Address: telecommuterc.com
	Remote Address 192.168.4.15

17 System Monitor

17.1 Overview

Use the **System Monitor** screens to look at network traffic status and statistics of the WAN, LAN interfaces and NAT.

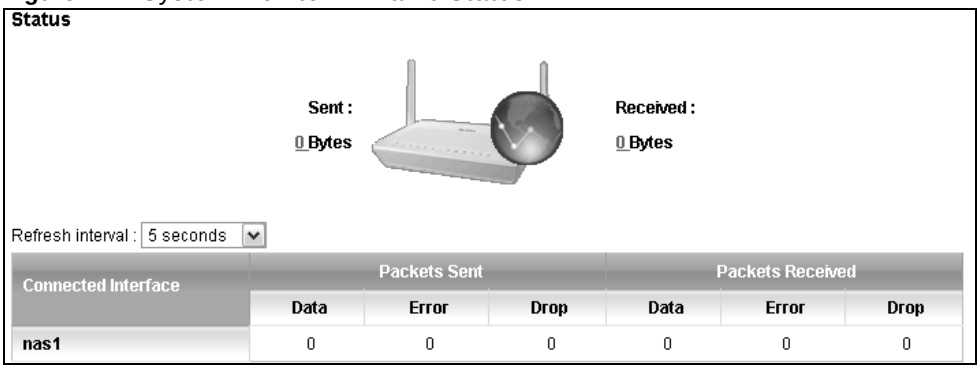
17.1.1 What You Can Do in this Chapter

- Use the **WAN** screen to view the WAN traffic statistics (Section 17.2 on page 223).
- Use the **LAN** screen to view the LAN traffic statistics (Section 17.3 on page 224).
- Use the **NAT** screen to view the NAT status of the ZyXEL Device's client(s) (Section 17.4 on page 225).

17.2 The WAN Status Screen

Click **System Monitor > Traffic Status** to open the **WAN** screen. You can view the WAN traffic statistics in this screen.

Figure 117 System Monitor > Traffic Status > WAN



The following table describes the fields in this screen.

Table 74 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Status	This shows the number of bytes received and sent through the WAN interface of the ZyXEL Device.
Refresh Interval	Select how often you want the ZyXEL Device to update this screen from the drop-down list box.
Connected Interface	This shows the name of the WAN interface that is currently connected.

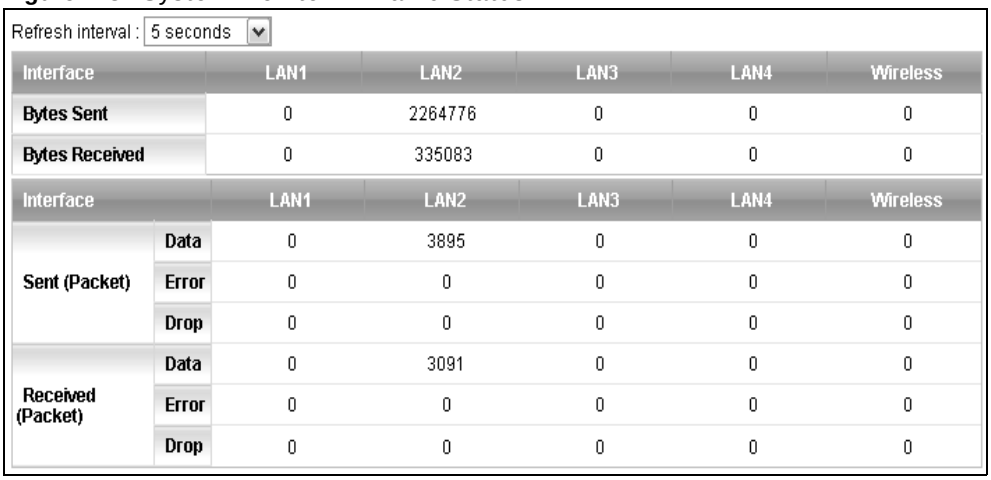
Table 74 System Monitor > Traffic Status > WAN

LABEL	DESCRIPTION
Packets Sent	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.
Packets Received	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

17.3 The LAN Status Screen

Click **System Monitor > Traffic Status > LAN** to open the following screen. You can view the LAN traffic statistics in this screen.

Figure 118 System Monitor > Traffic Status > LAN



The following table describes the fields in this screen.

Table 75 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the ZyXEL Device to update this screen from the drop-down list box.
Interface	This shows the LAN or WLAN interface.
Bytes Sent	This indicates the number of bytes transmitted on this interface.
Bytes Received	This indicates the number of bytes received on this interface.
Interface	This shows the LAN or WLAN interface.
Sent (Packet)	
Data	This indicates the number of transmitted packets on this interface.
Error	This indicates the number of frames with errors transmitted on this interface.
Drop	This indicates the number of outgoing packets dropped on this interface.

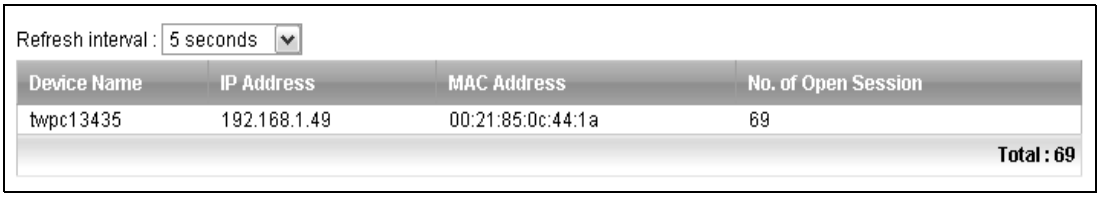
Table 75 System Monitor > Traffic Status > LAN

LABEL	DESCRIPTION
Received (Packet)	
Data	This indicates the number of received packets on this interface.
Error	This indicates the number of frames with errors received on this interface.
Drop	This indicates the number of received packets dropped on this interface.

17.4 The NAT Status Screen

Click **System Monitor > Traffic Status > NAT** to open the following screen. You can view the NAT status of the ZyXEL Device's client(s) in this screen.

Figure 119 System Monitor > Traffic Status > NAT



The following table describes the fields in this screen.

Table 76 System Monitor > Traffic Status > NAT

LABEL	DESCRIPTION
Refresh Interval	Select how often you want the ZyXEL Device to update this screen from the drop-down list box.
Device Name	This shows the name of the client.
IP Address	This shows the IP address of the client.
MAC Address	This shows the MAC address of the client.
No. of Open Session	This shows the number of NAT sessions used by the client.

18

User Account

18.1 Overview

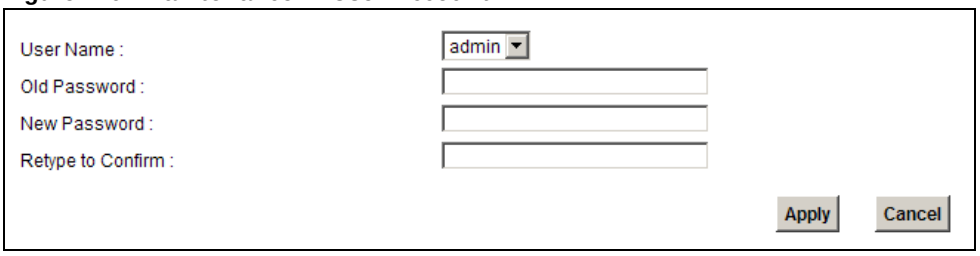
You can configure system password for different user accounts in the **User Account** screen.

18.2 The User Account Screen

Use the **User Account** screen to configure system password.

Click **Maintenance > User Account** to open the following screen.

Figure 120 Maintenance > User Account



The following table describes the labels in this screen.

Table 77 Maintenance > User Account

LABEL	DESCRIPTION
User Name	You can configure the password for the admin or user account. Select **admin** or **user** from the drop-down list box.
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays a (*) for each character you type. After you change the password, use the new password to access the ZyXEL Device.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

19

Remote MGMT

19.1 Overview

Remote MGMT allows you to manage your ZyXEL Device from a remote location through the following interfaces:

- LAN and WLAN
- WAN only

Note: The ZyXEL Device is managed using the web configurator.

19.1.1 What You Need to Know

The following terms and concepts may help as you read this chapter

TR-064

TR-064 is a LAN-Side DSL CPE Configuration protocol defined by the DSL Forum. TR-064 is built on top of UPnP. It allows the users to use a TR-064 compliant CPE management application on their computers from the LAN to discover the CPE and configure user-specific parameters, such as the username and password.

SSH/SCP/SFTP

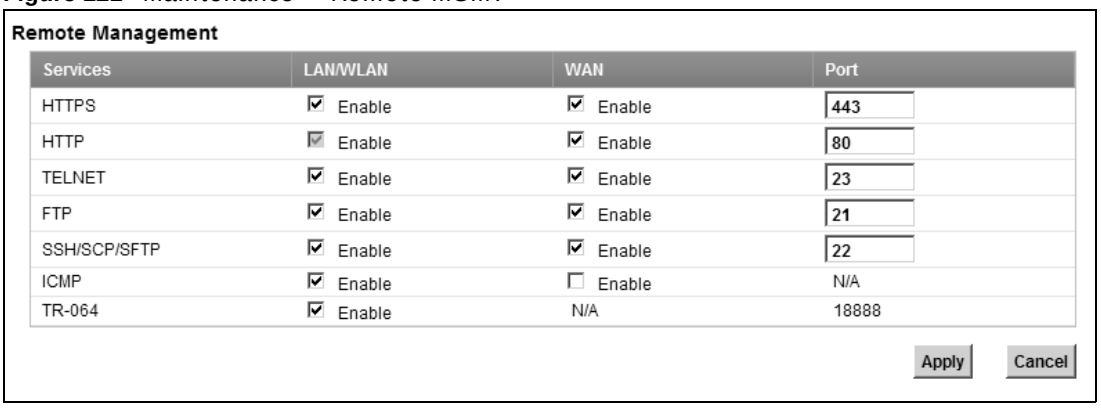
Secure Shell (SSH) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. The following file transfer methods use SSH:

- **Secure Copy (SC)** is a secure way of transferring files between computers. It uses port 22.
- **SSH File Transfer Protocol or Secure File Transfer Protocol (SFTP)** is an old way of transferring files between computers. It uses port 22.

19.2 The Remote MGMT Screen

Use this screen to decide what services you may use to access which ZyXEL Device interface. Click **Maintenance > Remote MGMT** to open the following screen.

Figure 121 Maintenance > Remote MGMT



The following table describes the fields in this screen.

Table 78 Maintenance > Remote MGMT

LABEL	DESCRIPTION
Services	This is the service you may use to access the ZyXEL Device.
LAN/WLAN	Select the **Enable** check box for the corresponding services that you want to allow access to the ZyXEL Device from the LAN and WLAN.
WAN	Select the **Enable** check box for the corresponding services that you want to allow access to the ZyXEL Device from the WAN.
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

20 System

20.1 Overview

You can configure system settings, including the host name, domain name and the inactivity time-out interval in the **System** screen.

20.1.1 What You Need to Know

The following terms and concepts may help as you read this chapter.

Domain Name

This is a network address that identifies the owner of a network connection. For example, in the network address “www.zyxel.com/support/files”, the domain name is “www.zyxel.com”.

20.2 The System Screen

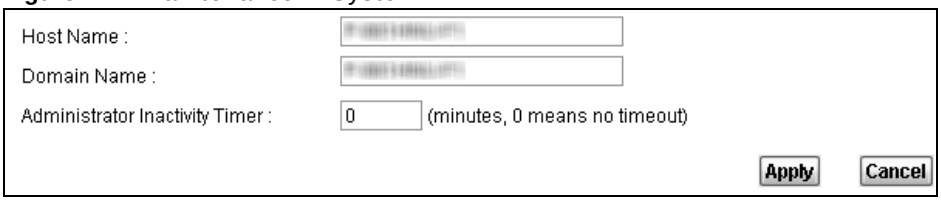
Use the **System** screen to configure the system’s host name, domain name, and inactivity time-out interval.

The **Host Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name". Find the system name of your Windows computer.

In Windows XP, click **start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyXEL Device **System Name**.

Click **Maintenance > System** to open the following screen.

Figure 122 Maintenance > System



The following table describes the labels in this screen.

Table 79 Maintenance > System

LABEL	DESCRIPTION
Host Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click this to save your changes back to the ZyXEL Device.
Cancel	Click this to begin configuring this screen afresh.

21

Time Setting

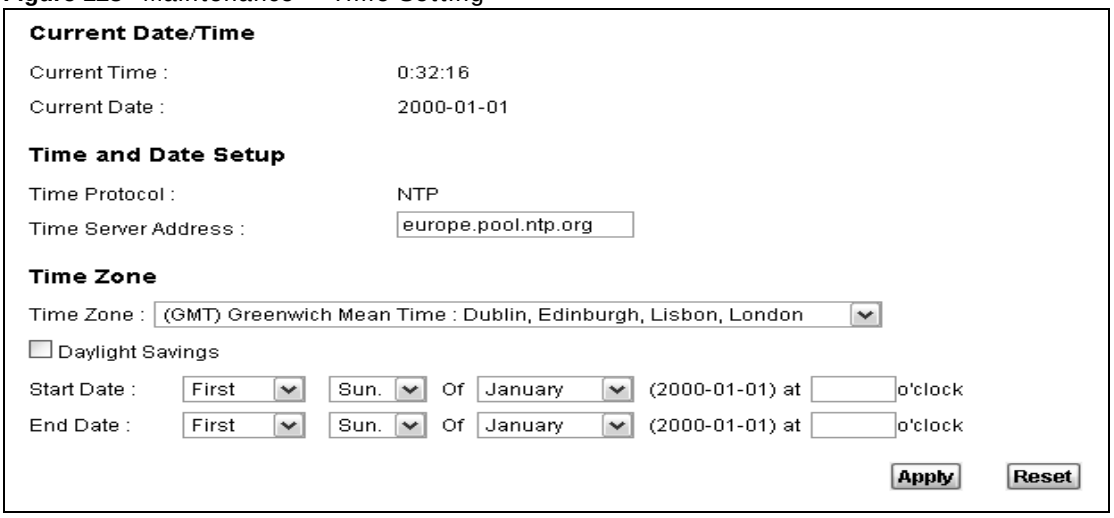
21.1 Overview

You can configure the system's time and date in the **Time Setting** screen.

21.2 The Time Setting Screen

To change your ZyXEL Device's time and date, click **Maintenance > Time Setting**. The screen appears as shown. Use this screen to configure the ZyXEL Device's time based on your local time zone.

Figure 123 Maintenance > Time Setting



The following table describes the fields in this screen.

Table 80 Maintenance > Time Setting

LABEL	DESCRIPTION
Current Date/Time	
Current Time	This field displays the time of your ZyXEL Device.
Current Date	This field displays the date of your ZyXEL Device.
Time and Date Setup	
Get from Time Server	The ZyXEL Device get the time and date from the time server you specified below.
Time Protocol	This shows the time service protocol that your time server sends when you turn on the ZyXEL Device.

Table 80 Maintenance > Time Setting (continued)

LABEL	DESCRIPTION
Time Server Address	Enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and type **2** in the **o'clock** field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type **2** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and type **2** in the **o'clock** field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type **2** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

22

Log Setting

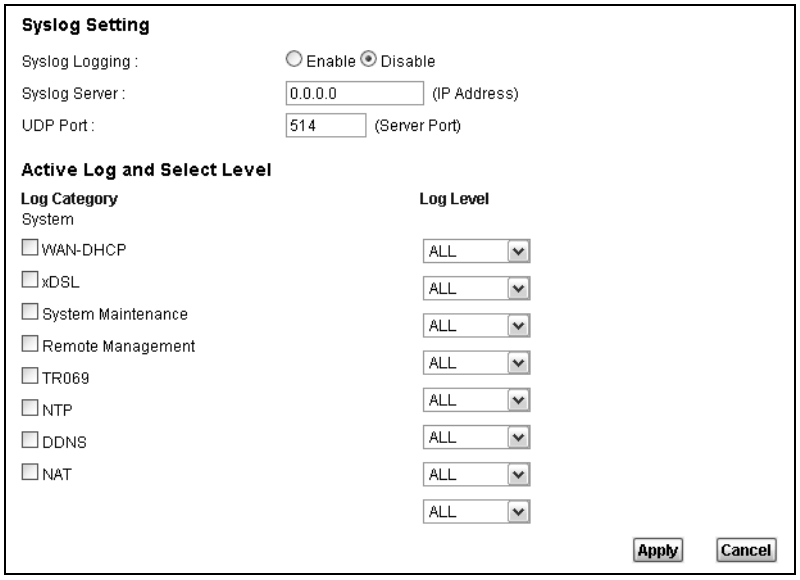
22.1 Overview

You can configure where the ZyXEL Device sends logs and which logs and/or immediate alerts the ZyXEL Device records in the **Log Setting** screen.

22.2 The Log Setting Screen

To change your ZyXEL Device's log settings, click **Maintenance > Log Setting**. The screen appears as shown.

Figure 124 Maintenance > Log Setting



The following table describes the fields in this screen.

Table 81 Maintenance > Log Setting

LABEL	DESCRIPTION
Syslog Logging	The ZyXEL Device sends a log to an external syslog server. Select the **Enable** check box to enable syslog logging.
Syslog Server	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
UDP Port	Enter the port number used by the syslog server.
Active Log and Select Level	
Log Category	Select the categories of logs that you want to record.
Log Level	Select the severity level of logs that you want to record. If you want to record all logs, select **ALL**.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

23

Firmware Upgrade

23.1 Overview

This chapter explains how to upload new firmware to your ZyXEL Device. You can download new firmware releases from your nearest ZyXEL FTP site (or www.zyxel.com) to use to upgrade your device's performance.

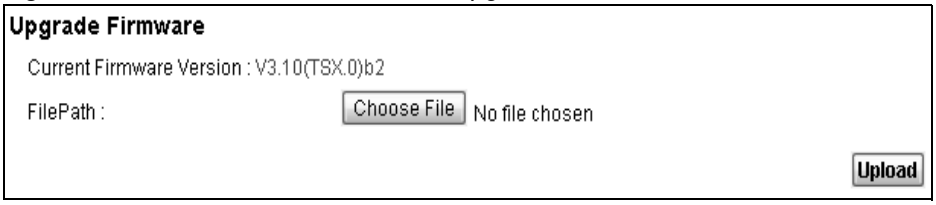
Only use firmware for your device's specific model. Refer to the label on the bottom of your ZyXEL Device.

23.2 The Firmware Screen

Click **Maintenance > Firmware Upgrade** to open the following screen. The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Do NOT turn off the ZyXEL Device while firmware upload is in progress!

Figure 125 Maintenance > Firmware Upgrade



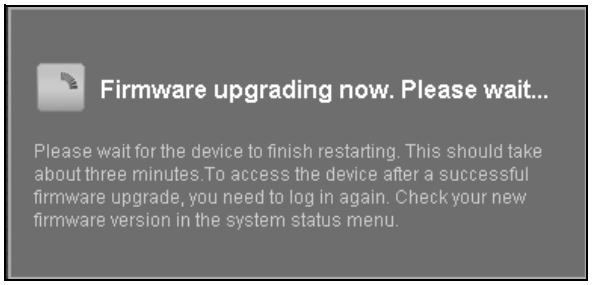
The following table describes the labels in this screen.

Table 82 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Current Firmware Version	This is the present Firmware version.
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click this to begin the upload process. This process may take up to two minutes.

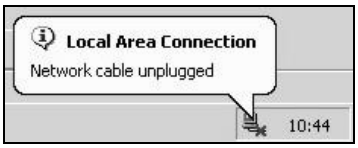
After you see the firmware updating screen, wait two minutes before logging into the ZyXEL Device again.

Figure 126 Firmware Uploading


Firmware upgrading now. Please wait...
Please wait for the device to finish restarting. This should take about three minutes.To access the device after a successful firmware upgrade, you need to log in again. Check your new firmware version in the system status menu.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

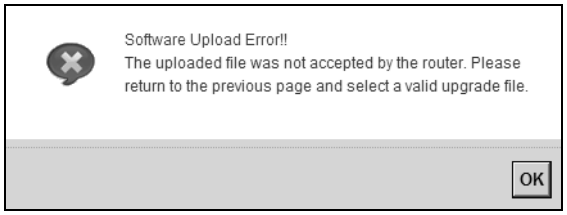
Figure 127 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **Status** screen.

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Firmware Upgrade** screen.

Figure 128 Error Message


Software Upload Error!!
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file.
OK

24

Backup/Restore

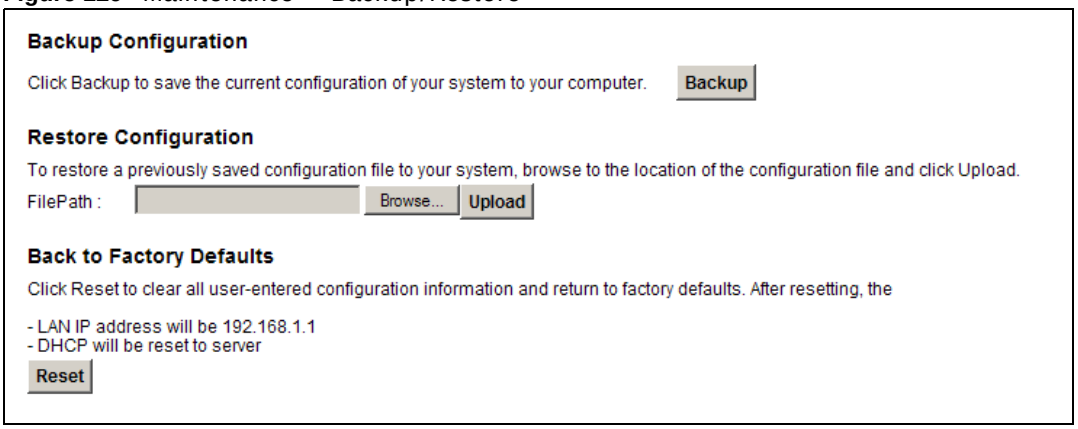
24.1 Overview

The **Backup / Restore** screen allows you to backup and restore device configurations. You can also reset your device settings back to the factory default.

24.2 The Backup/Restore Screen

Click **Maintenance > Backup / Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears in this screen, as shown next.

Figure 129 Maintenance > Backup/Restore


Backup Configuration
Click Backup to save the current configuration of your system to your computer.
Backup
Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
FilePath :
Browse...
Upload
Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server
Reset

Backup Configuration

Backup Configuration allows you to back up (save) the ZyXEL Device's current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyXEL Device's current configuration to your computer.

Restore Configuration

Restore Configuration allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device.

Table 83 Restore Configuration

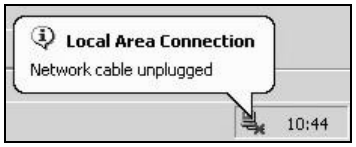
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click this to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click this to begin the upload process.
Reset	Click this to reset your device settings back to the factory default.

Do not turn off the ZyXEL Device while configuration file upload is in progress.

After the ZyXEL Device configuration has been restored successfully, the login screen appears. Login again to restart the ZyXEL Device.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 130 Network Temporarily Disconnected



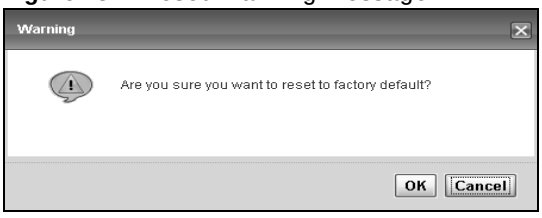
If you restore the default configuration, you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See Appendix B on page 273 for details on how to set up your computer's IP address.

If the upload was not successful, an error screen will appear. Click **OK** to go back to the **Configuration** screen.

Reset to Factory Defaults

Click the **Reset** button to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults. The following warning screen appears.

Figure 131 Reset Warning Message



Wait until the ZyXEL Device's login screen appears. You can also press the **RESET** button on the rear panel to reset the factory defaults of your ZyXEL Device. Refer to Section 1.6 on page 25 for more information on the **RESET** button.

24.3 The Reboot Screen

System restart allows you to reboot the ZyXEL Device remotely without turning the power off. You may need to do this if the ZyXEL Device hangs, for example.

Click **Maintenance > Reboot**. Click the **Reboot** button to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

25 Diagnostic

25.1 Overview

You can use different diagnostic methods to test a connection and see the detailed information. These read-only screens display information to help you identify problems with the ZyXEL Device.

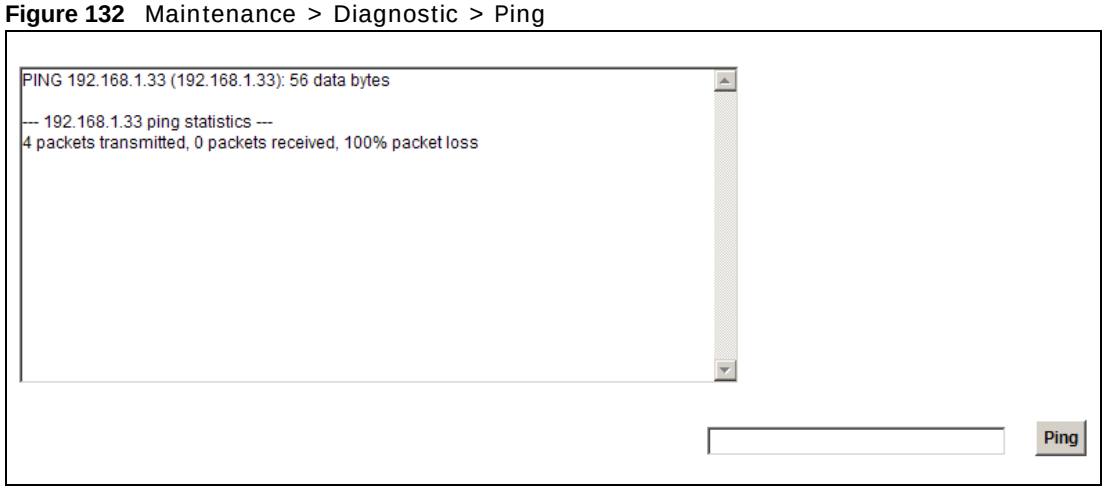
25.1.1 What You Can Do in this Chapter

- Use the **Ping** screen to ping an IP address and see the ping statistics (Section 25.2 on page 243).
- Use the **DSL Line** screen to check or reset your DSL connection (Section 25.3 on page 244).

25.2 The Ping Screen

Use this screen to ping an IP address. Click **Maintenance > Diagnostic** to open the **Ping** screen shown next.

Figure 132 Maintenance > Diagnostic > Ping


PING 192.168.1.33 (192.168.1.33): 56 data bytes
--- 192.168.1.33 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
Ping

The following table describes the fields in this screen.

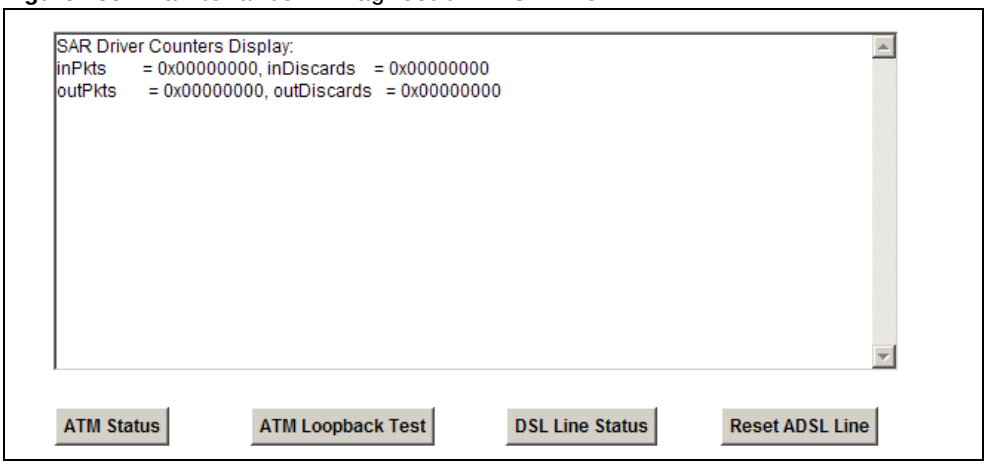
Table 84 Maintenance > Diagnostic > Ping

LABEL	DESCRIPTION
Ping	Type the IP address of a computer that you want to ping in order to test a connection. Click **Ping** and the ping statistics will show in the diagnostic.

25.3 The DSL Line Screen

Click **Maintenance > Diagnostic > DSL Line** to open the screen shown next.

Figure 133 Maintenance > Diagnostic > DSL Line



The following table describes the fields in this screen.

Table 85 Maintenance > Diagnostic > DSL Line

ITEM	DESCRIPTION
ATM Status	Click this button to view your DSL connection's Asynchronous Transfer Mode (ATM) statistics. ATM is a networking technology that provides high-speed data transfer. ATM uses fixed-size packets of information called cells. With ATM, a high QoS (Quality of Service) can be guaranteed. The (Segmentation and Reassembly) SAR driver translates packets into ATM cells. It also receives ATM cells and reassembles them into packets. These counters are set back to zero whenever the device starts up. **inPkts** is the number of good ATM cells that have been received. **inDiscards** is the number of received ATM cells that were rejected. **outPkts** is the number of ATM cells that have been sent. **outDiscards** is the number of ATM cells sent that were rejected.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The ZyXEL Device sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the ZyXEL Device. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.

Table 85 Maintenance > Diagnostic > DSL Line

ITEM	DESCRIPTION
DSL Line Status	Click this button to view statistics about the DSL connections. 1. **noise margin downstream** is the signal to noise ratio for the downstream part of the connection (coming into the ZyXEL Device from the ISP). It is measured in decibels. The higher the number the more signal and less noise there is. 2. **output power upstream** is the amount of power (in decibels) that the ZyXEL Device is using to transmit to the ISP. 3. **attenuation downstream** is the reduction in amplitude (in decibels) of the DSL signal coming into the ZyXEL Device from the ISP. Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each called tones. The rest of the display is the line's bit allocation. This is displayed as the number (in hexadecimal format) of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support certain ADSL transmission rates, and possibly to determine whether particular specific types of interference or line attenuation exist. Refer to the ITU-T G.992.1 recommendation for more information on DMT. The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15. There will be some tones without any bits as there has to be space between the upstream and downstream channels.

Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example:
	
	`"Start to reset ADSL`
	
	`Loading ADSL modem F/W...`
	
	`Reset ADSL Line Successfully!"`

26

Troubleshooting

26.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyXEL Device Access and Login
- Internet Access
- Wireless Internet Access
- USB Device Connection
- UPnP

26.2 Power, Hardware Connections, and LEDs

The ZyXEL Device does not turn on. None of the LEDs turn on.

1. Make sure the ZyXEL Device is turned on.
2. Make sure you are using the power adaptor or cord included with the ZyXEL Device.
3. Make sure the power adaptor or cord is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the ZyXEL Device off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See page 255.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Turn the ZyXEL Device off and on.

5 If the problem continues, contact the vendor.

26.3 ZyXEL Device Access and Login

I forgot the IP address for the ZyXEL Device.

1 The default IP address is 192.168.1.1.

2 If you changed the IP address and have forgotten it, you might get the IP address of the ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 25.

I forgot the password.

1 The default admin and user password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 1.6 on page 25.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.1.
- If you changed the IP address - see page 145, use the new IP address.
- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the ZyXEL Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix C on page 303.

4 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See Section 1.6 on page 25.

5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the ZyXEL Device using another service, such as Telnet. If you can access the ZyXEL Device, check the remote management settings and firewall rules to find out why the ZyXEL Device does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to an **ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the ZyXEL Device.

1 Make sure you have entered the user name and password correctly. The default user name is **admin**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.

3 Turn the ZyXEL Device off, wait for one minute and turn it back on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 26.2 on page 247.

I cannot telnet to the ZyXEL Device.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

I cannot use FTP to upload / download the configuration file. / I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

26.4 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and page 255.
2. Make sure you entered your ISP account information correctly. These fields are case-sensitive, so make sure [Caps Lock] is not on.
3. If you are trying to access the Internet wirelessly, make sure the wireless settings in the wireless client are the same as the settings in the AP.
4. If you are trying to access the Internet wirelessly, make sure you have enabled the wireless LAN by the **WPS/WLAN** button or the **Network Setting > Wireless > General** screen.
5. Turn the ZyXEL Device off. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
6. If the problem continues, contact your ISP.

I cannot access the Internet through a DSL connection.

1. Make sure you configured a proper DSL WAN connection with the Internet account information provided by your ISP.
2. If you set up a WAN connection using bridging service (all LAN ports and WLAN BSSs are bridged to one WAN connection), make sure you turn off the DHCP feature in the **Home Networking** screen to have the clients get WAN IP addresses directly from your ISP's DHCP server.

I cannot create multiple connections of the same type.

Your WAN interface must enable VLAN and fill each WAN connection with different VLAN IDs.

I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and page 255.
2. Turn the ZyXEL Device off, wait for one minute and turn it back on.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check page 255. If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Turn the ZyXEL Device off, wait for one minute and turn it back on.

3 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Check the settings for QoS. If it is disabled, you might consider activating it. If it is enabled, you might consider raising or lowering the priority for some applications.

26.5 Wireless Internet Access

What factors may cause intermittent or unstabled wireless connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.
- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless connection, you can:

- Move your wireless device closer to the AP if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the AP where there are minimum obstacles (such as walls and ceilings) between the AP and the wireless client.
- Reduce the number of wireless clients connecting to the same AP simultaneously, or add additional APs if necessary.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

- Position the antennas for best reception. If the AP is placed on a table or floor, point the antennas upwards. If the AP is placed at a high position, point the antennas downwards. Try pointing the antennas in different directions and check which provides the strongest signal to the wireless clients.

What wireless security modes does my ZyXEL Device support?

Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network.

The available security modes in your ZyXEL device are as follows:

- **WPA2-PSK:** (recommended) This uses a pre-shared key with the WPA2 standard.
- **WPA-PSK:** This has the device use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.
- **WPA2:** WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA. It requires the use of a RADIUS server and is mostly used in business networks.
- **WPA:** Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. It requires the use of a RADIUS server and is mostly used in business networks.
- **WEP:** Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.

26.6 USB Device Connection

The ZyXEL Device fails to detect my USB device.

1. Disconnect the USB device.
2. Reboot the ZyXEL Device.
3. If you are connecting a USB hard drive that comes with an external power supply, make sure it is connected to an appropriate power source that is on.
4. Re-connect your USB device to the ZyXEL Device.
5. If the problem persists, make sure the option **File Sharing Services(SMB)** is enabled in the **Web Configurator** - see Section 3.5.1.1 on page 51.

The USB device is properly connected, but I cannot see it when I open My Computer

1 If the USB device is connected to the ZyXEL Device, it won't be listed directly under My Computer in Windows. To access the USB device - see Section 3.5.2 on page 54.

2 If you still cannot see the specific share you are trying to access, open the **Web Configurator** and go to **Network Setting > File Sharing**. Make sure that the share has a check below the symbol **"#"**. This means that the USB Device is enabled for sharing - see Section 3.5.1 on page 51.

I can see the USB device but I cannot access it.

1 Restart the computer and try to access the device again. Make sure you have the correct password

2 If the share's settings have been set to **Private**, you may not have permission to see the share's content. Open the **Web Configurator** and make sure you add your user to the list **Allow Users** in the **Add/Edit Share** screen - see Section 3.5.1.3 on page 52.

3 Make sure you have the correct password. If you have forgotten the password, delete the username, restart the computer, add the username again and try to access the device.

26.7 UPnP

When using UPnP and the ZyXEL Device reboots, my computer cannot detect UPnP and refresh **My Network Places > Local Network**.

1 Disconnect the Ethernet cable from the ZyXEL Device's LAN port or from your computer.

2 Re-connect the Ethernet cable.

The **Local Area Connection** icon for UPnP disappears in the screen.

Restart your computer.

I cannot open special applications such as white board, file transfer and video when I use the MSN messenger.

1 Wait more than three minutes.

2 Restart the applications.

27

Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

LEDs (Lights)

The following table describes the LEDs.

None of the LEDs are on if the ZyXEL Device is not receiving power.

Table 86 LED Descriptions

LED	NAME	COLOR	STATUS	DESCRIPTION
	POWER	Green	On	The ZyXEL Device is receiving power and ready for use.
			Blinking	The ZyXEL Device is self-testing.
		Red	On	The ZyXEL Device detected an error while self-testing, or there is a device malfunction.
		Off		The ZyXEL Device is not receiving power.
	ETHERNET1-4	Green	On	The ZyXEL Device has an Ethernet connection with a device on the Local Area Network (LAN).
			Blinking	The ZyXEL Device is sending/receiving data to/from the LAN.
		Off		The ZyXEL Device does not have an Ethernet connection with the LAN.
	WLAN/WPS	Green	On	The wireless network is activated and is operating in IEEE 802.11b/g/n mode.
			Blinking	The ZyXEL Device is communicating with other wireless clients.
		Orange	Blinking	The WPS connection is being configured.
		Off		The wireless network is not activated.
	DSL	Green	On	This light applies when the ZyXEL Device is in DSL WAN mode. The DSL line is up.
			Blinking	The ZyXEL Device is attempting to synchronize DSL signal.
		Off		The DSL line is down.
	INTERNET	Green	On	The ZyXEL Device has an IP connection but no traffic. Your device has a WAN IP address (either static or assigned by a DHCP server), PPP negotiation was successfully completed (if used).
			Blinking	The ZyXEL Device is sending or receiving IP traffic.
		Red	On	The ZyXEL Device attempted to make an IP connection but failed. Possible causes are no response from a DHCP server, no PPPoE response, PPPoE authentication failed.
		Off		The ZyXEL Device does not have an IP connection.

Table 86 LED Descriptions

LED	NAME	COLOR	STATUS	DESCRIPTION
	USB	Green	On	The ZyXEL Device recognizes a USB connection but there is no traffic.
			Blinking	The ZyXEL Device is sending/receiving data to/from the USB device connected to it.
		Off		The ZyXEL Device does not detect a USB connection.

Table 87 Hardware Specifications

Power Specification	12V 1.0A DC
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
RESET Button	Restores factory defaults
WLAN/WPS Button	1 second: Turn on or off WLAN 5 seconds: Start WPS
Operation Temperature	0º C ~ 40º C
Storage Temperature	-25º ~ 65º C
Operation Humidity	20% ~ 90% RH
Storage Humidity	20% ~ 90% RH

Firmware Specifications

Table 88 Firmware Specifications

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default User Name	admin
Default Password	1234
DHCP Server IP Pool	Starting Address: 192.168.1.33 Size: 32
Static DHCP Addresses	10
Static Routes	16
Device Management	Use the web configurator to easily configure the rich range of features on the ZyXEL Device.
Wireless Functionality (wireless devices only)	Allow the IEEE 802.11n, IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the ZyXEL Device wirelessly. Enable wireless security (WEP, WPA(2), WPA(2)-PSK) and/or MAC filtering to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator, an HTTP/FTP/SCP/SFTP tool to put it on the ZyXEL Device. Note: Only upload firmware for your specific model!
Configuration Backup & Restoration	Make a copy of the ZyXEL Device's configuration. You can put it back on the ZyXEL Device later if you decide to revert back to an earlier configuration.

Table 88 Firmware Specifications (continued)

Network Address Translation (NAT)	Each computer on your network must have its own unique IP address. Use NAT to convert your public IP address(es) to multiple private IP addresses for the computers on your network.
Port Forwarding	If you have a server (mail or web server for example) on your network, you can use this feature to let people access it from the Internet.
DHCP (Dynamic Host Configuration Protocol)	Use this feature to have the ZyXEL Device assign IP addresses, an IP default gateway and DNS servers to computers on your network.
Dynamic DNS Support	With Dynamic DNS (Domain Name System) support, you can use a fixed URL, www.zyxel.com for example, with a dynamic IP address. You must register for this service with a Dynamic DNS service provider.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The ZyXEL Device supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your ZyXEL Device. You can also set the time manually. These dates and times are then used in logs.
Logs	Use logs for troubleshooting. You can send logs from the ZyXEL Device to an external syslog server.
Universal Plug and Play (UPnP)	A UPnP-enabled device can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.
Firewall	Your device has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.
QoS (Quality of Service)	You can efficiently manage traffic on your network by reserving bandwidth and giving priority to certain types of traffic and/or to particular computers.
Remote Management	This allows you to decide whether a service (HTTP or FTP traffic for example) from a computer on a network (LAN or WAN for example) can access the ZyXEL Device. • Via HTTP/Telnet/SSH/SCP/SFTP • Configurable port number • Firmware upgrade via HTTP
PPPoE Support (RFC2516)	PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on your device is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.
Multiple PVC (Permanent Virtual Circuits) Support	Your device supports one Permanent Virtual Circuits (PVCs).
Packet Filters	Your device's packet filtering function allows added network security and management.

Table 88 Firmware Specifications (continued)

ADSL Standards	ANSI T1.413 Issue 2 ETSI ADSL over ISDN ITU G.dmt (G.992.1) Annex A,B ITU G.dmt.bis (G.992.3) (ADSL2) Annex A, B, I, J, L, M ITU G.dmt.plus (G.992.5) (ADSL2+) Annex A, B, I, J RE-ADSL (Reach-Extended ADSL) SRA (Seamless Rate Adaption) Auto-negotiating rate adaption EOC specified in ITU-T G.992.1 Support 7 PVC I.610 F4/F5 OAM VC-based and LLC-based multiplexing Multi-protocol over AAL5 (RFC2684/1483) PPP over ATM/AAL5 (RFC2364) Traffic shaping (CBR, VBR-rt/nrt, UBR) PPPoE (RFC2516) EOC specified in ITU-T G.992.1 ADSL physical connection AAL5 (ATM Adaptation Layer type 5)
Other Protocol Support	Transparent bridging for unsupported network layer protocols ICMP ATM QoS IP Multicasting IGMP v1, v2 IGMP Proxy/Snooping IGMP fast leave
Management	Embedded Web Configurator CLI (Command Line Interpreter) Firmware upgrade via HTTP Configuration file extraction using CLI, SFTP, SCP and TR-069. Factory reset vis CLI, TR-069 and physical button Telnet for remote management Remote Firmware Upgrade Syslog TR-069, TR-064, TR-068v2, TR098, TR-106

Wireless Features

Table 89 Wireless Features

External Antenna	The ZyXEL Device is equipped with two detachable antennas to provide a clear radio signal between the wireless stations and the access points.
Multiple SSID	Multiple SSID allows the ZyXEL Device to operate up to 4 different wireless networks simultaneously, each with independently configurable wireless and security settings.
MAC Address Filtering	Your device can check the MAC addresses of clients against a list of allowed MAC addresses.
WEP Encryption	WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.
Wi-Fi Protected Access	Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security standard. Key differences between WPA and WEP are user authentication and improved data encryption.

Table 89 Wireless Features

WPA2	WPA 2 is a wireless security standard that defines stronger encryption, authentication and key management than WPA.
WPS	Wi-Fi Protected Setup
Other Wireless Features	IEEE 802.11b/g/n Compliance Frequency Range: 2.4 GHz ISM Band Operating Frequency: • 2.412G~2.462GHz: (FCC) North America (CH1~CH11) • 2.412G~2.472GHz: (ETSI/TELEC) EU/Japan (CH1~CH13) Advanced Orthogonal Frequency Division Multiplexing (OFDM) Data Rates: • 802.11n: 6.5, 7.2, 13, 13.5, 14.4, 15, 19.5, 21.7, 26, 27, 28.9, 30, 39, 40.5, 43.3, 45, 52, 54, 57.8, 58.5, 60, 65, 72.2, 78, 81, 86.7, 90, 104, 108, 115.6, 117, 120, 121.5, 130, 135, 144.4, 150, 162, 180, 216, 240, 243, 270, 300 Mbps • 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps • 802.11b: 1, 2, 5.5, 11Mbps Modulation Technique: • 802.11n: MIMO-OFDM (BPSK, QPSK, 16-QAM, 64-QAM) • 802.11g: OFDM (BPSK, QPSK, 16-QAM, 64-QAM) • 802.11b: CCK, DQPSK, DBPSK Turn on-off WLAN by **WLAN** button (press the **WLAN** button for one second to turn the WLAN on or turn off; five seconds to turn on WPS) WLAN bridge to LAN Up to 32 MAC Address filters Scheduling lets you set when the WLAN is on

The following list, which is not exhaustive, illustrates the standards supported in the ZyXEL Device.

Table 90 Standards Supported

STANDARD	DESCRIPTION
RFC 867	Daytime Protocol
RFC 868	Time Protocol
RFC 1112	IGMP v1
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1483	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 2236	Internet Group Management Protocol, Version 2
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5
RFC 2766	Network Address Translation - Protocol

Table 90 Standards Supported (continued)

STANDARD	DESCRIPTION
IEEE 802.11	Also known by the brand Wi-Fi, denotes a set of Wireless LAN/WLAN standards developed by working group 11 of the IEEE LAN/MAN Standards Committee (IEEE 802)
IEEE 802.11b	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11g	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11n	Uses the 2.4 gigahertz (GHz) band
IEEE 802.11d	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
802.1x	Port Based Network Access Control
IEEE 802.11e QoS	IEEE 802.11 e Wireless LAN for Quality of Service
ANSI T1.413, Issue 2	Asymmetric Digital Subscriber Line (ADSL) standard
G dmt(G.992.1)	G.992.1 Asymmetrical Digital Subscriber Line (ADSL) Transceivers
ITU G.992.1 (G.DMT)	ITU standard for ADSL using discrete multitone modulation
ITU G.992.2 (G. Lite)	ITU standard for ADSL using discrete multitone modulation
ITU G.992.3 (G.dmt.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates
ITU G.992.4 (G.lite.bis)	ITU standard (also referred to as ADSL2) that extends the capability of basic ADSL in data rates
ITU G.992.5 (ADSL2+)	ITU standard (also referred to as ADSL2+) that extends the capability of basic ADSL by doubling the number of downstream bits
RFC 2383	ST2+ over ATM Protocol Specification - UNI 3.1 Version
TR-069	TR-069 DSL Forum Standard for CPE Wan Management
TR-064	DSL Forum LAN-Side DSL CPE Configuration
1.363.5	Compliant AAL5 SAR (Segmentation And Re-assembly)

Wall-mounting Instructions

Do the following to hang your ZyXEL Device on a wall.

Note: See Table 87 on page 256 for the size of screws to use and how far apart to place them.

1 Locate a high position on a wall that is free of obstructions. Use a sturdy wall.

2 Drill two holes for the screws. Make sure the distance between the centers of the holes matches what is listed in the product specifications appendix.

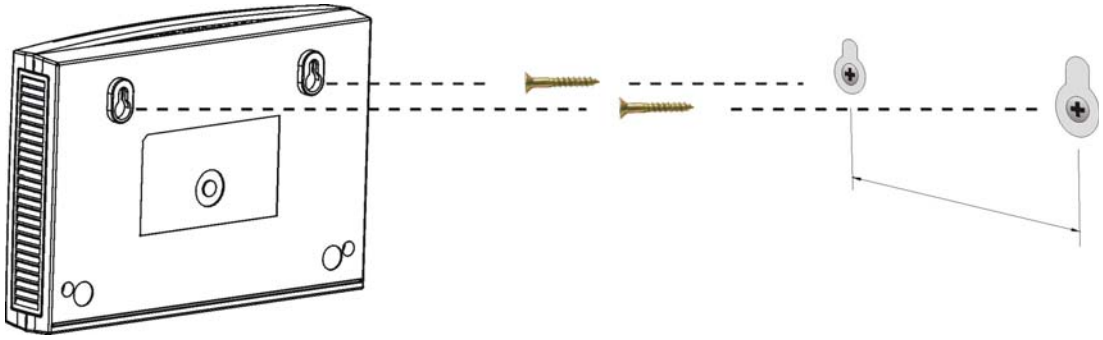
Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

3 Do not screw the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.

4 Make sure the screws are snugly fastened to the wall. They need to hold the weight of the ZyXEL Device with the connection cables.

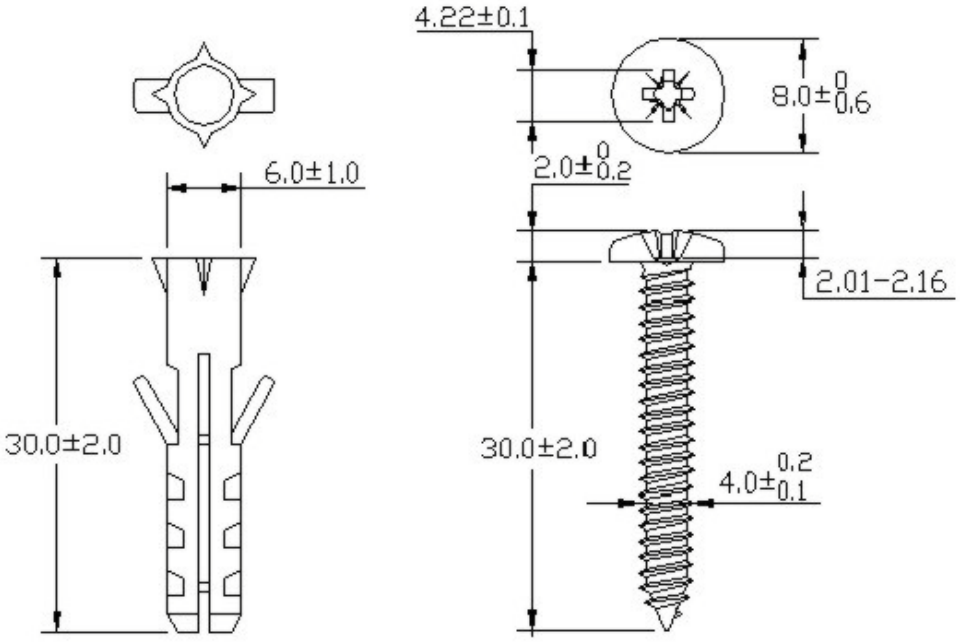
5 Align the holes on the back of the ZyXEL Device with the screws on the wall. Hang the ZyXEL Device on the screws.

Figure 134 Wall-mounting Example



The following are dimensions of an M4 tap screw and masonry plug used for wall mounting. All measurements are in millimeters (mm).

Figure 135 Masonry Plug and M4 Tap Screw



A

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (such as computers, servers, routers, and printers) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

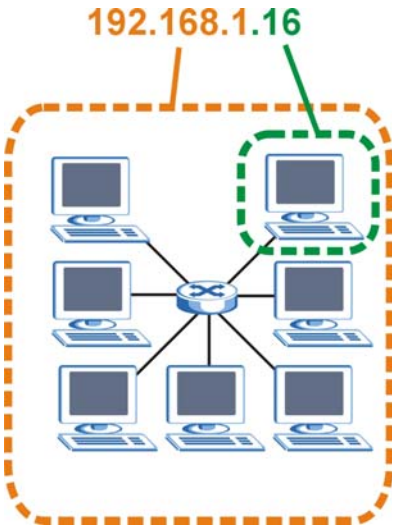
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 136 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 91 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 92 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 93 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 94 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224

Table 94 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

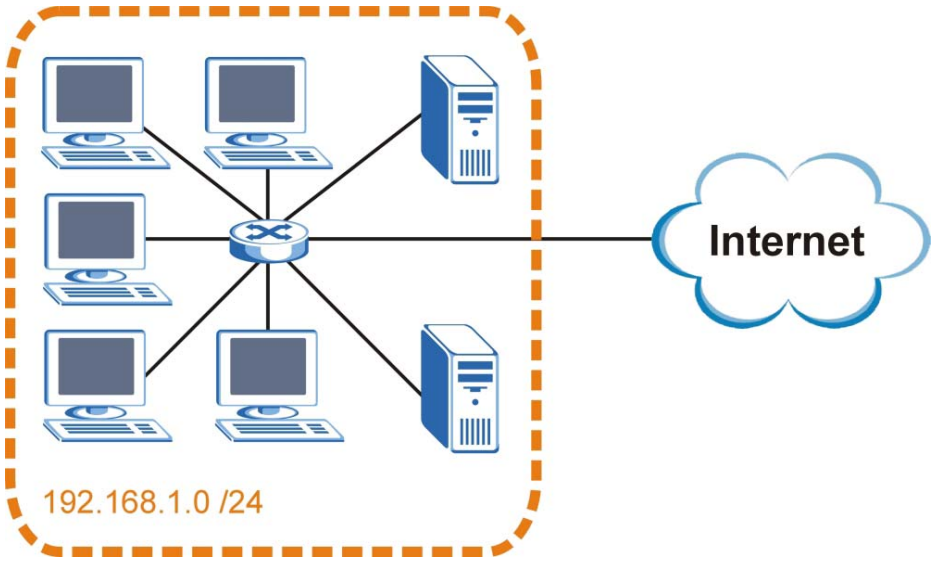
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of 2^8 – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 137 Subnetting Example: Before Subnetting

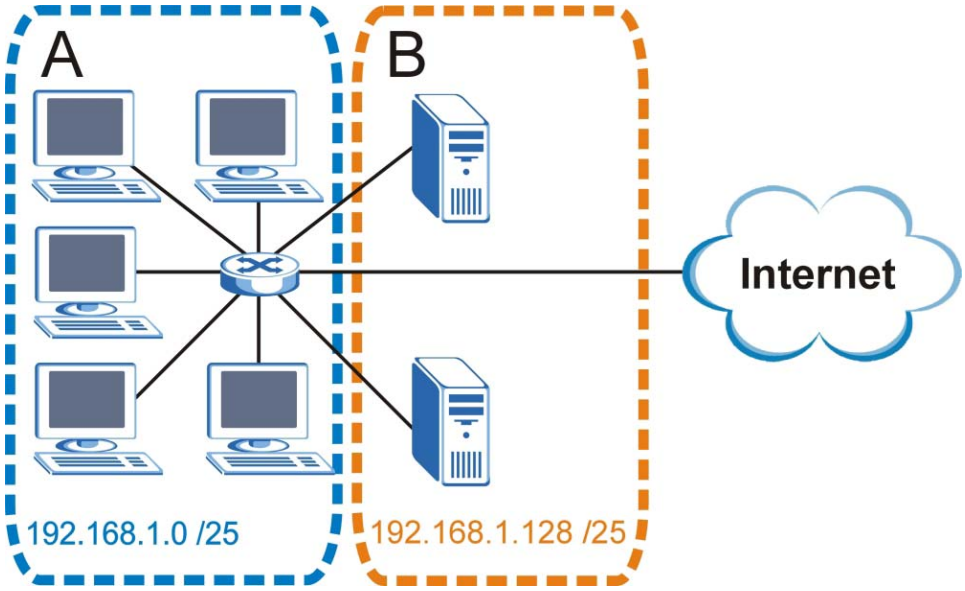


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 138 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of 2^7 – 2 or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 95 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 96 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 97 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 98 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 99 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191

Table 99 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 100 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 101 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyXEL Device.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

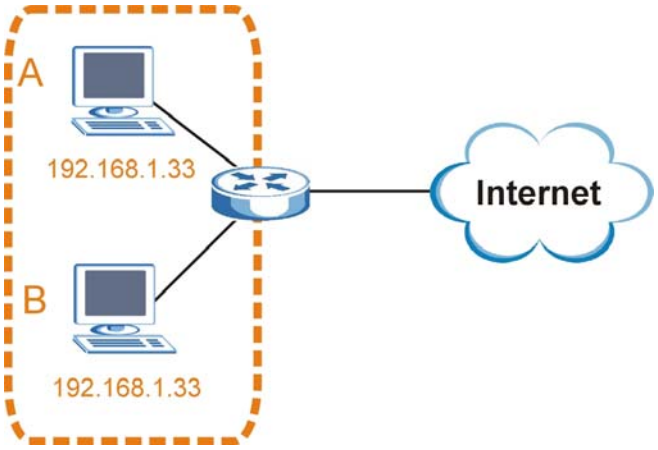
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

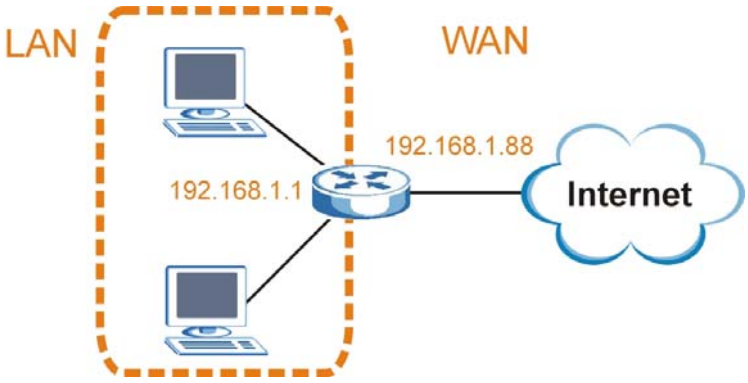
Figure 139 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

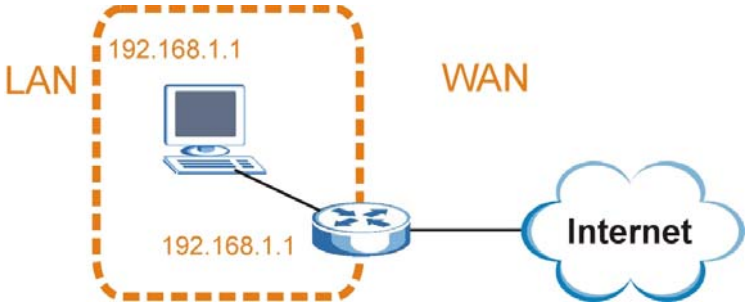
Figure 140 Conflicting Computer IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 141 Conflicting Computer and Router IP Addresses Example



B

Setting Up Your Computer's IP Address

Note: Your specific ZyXEL Device may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

In this appendix, you can set up an IP address for:

- Windows XP/NT/2000 on page 273
- Windows Vista on page 277
- Windows 7 on page 281
- Mac OS X: 10.3 and 10.4 on page 285
- Mac OS X: 10.5 on page 288
- Linux: Ubuntu 8 (GNOME) on page 292
- Linux: openSUSE 10.3 (KDE) on page 296

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

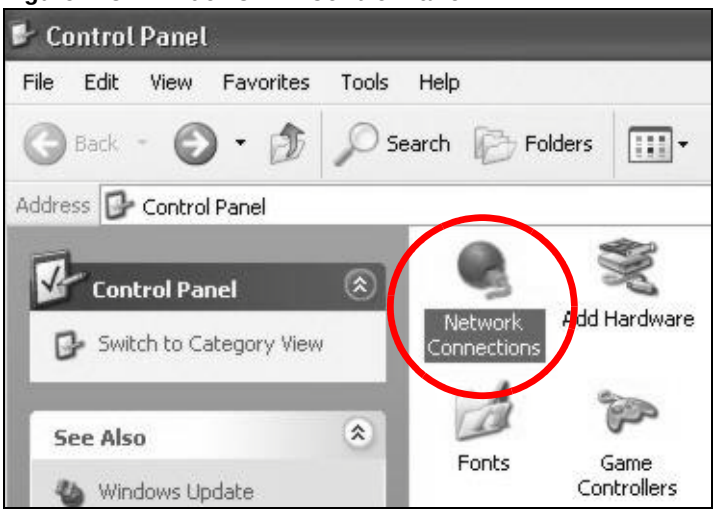
1 Click **Start** > **Control Panel**.

Figure 142 Windows XP: Start Menu



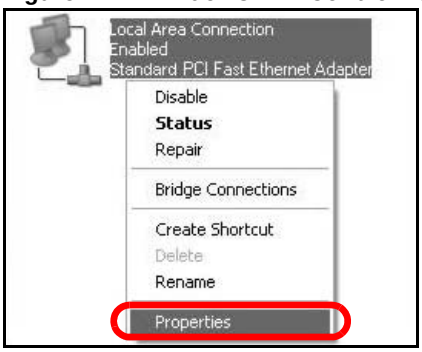
2 In the **Control Panel**, click the **Network Connections** icon.

Figure 143 Windows XP: Control Panel



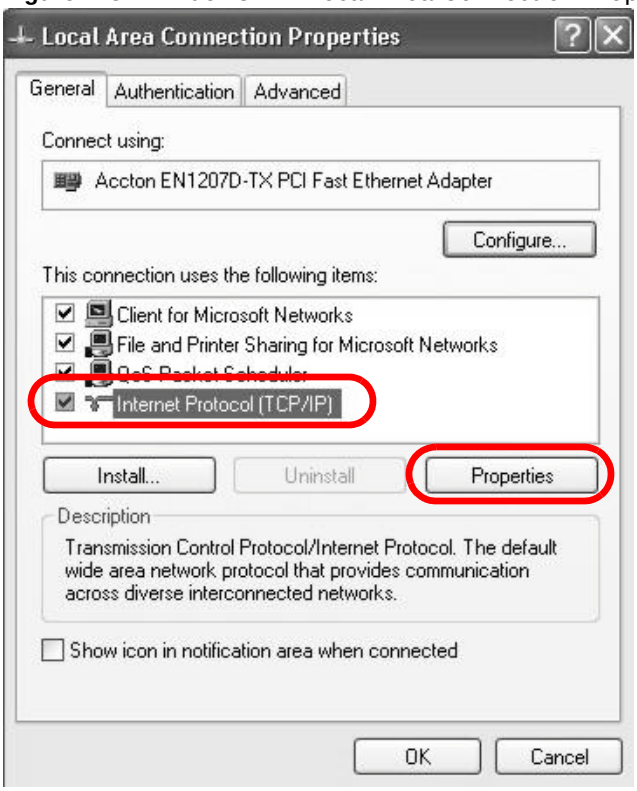
3 Right-click **Local Area Connection** and then select **Properties**.

Figure 144 Windows XP: Control Panel > Network Connections > Properties



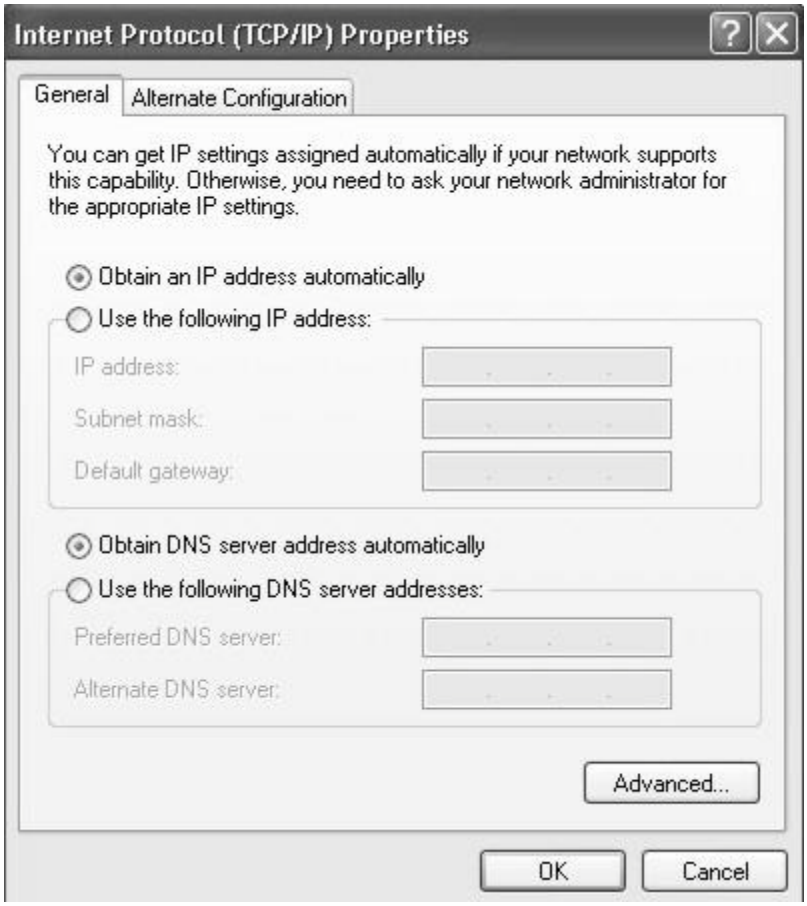
4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 145 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens.

Figure 146 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

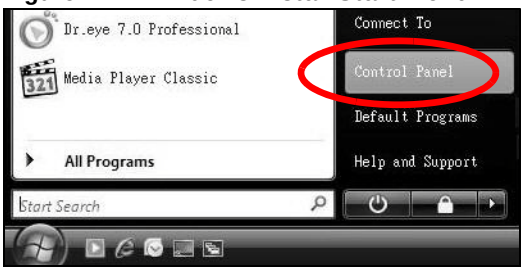
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

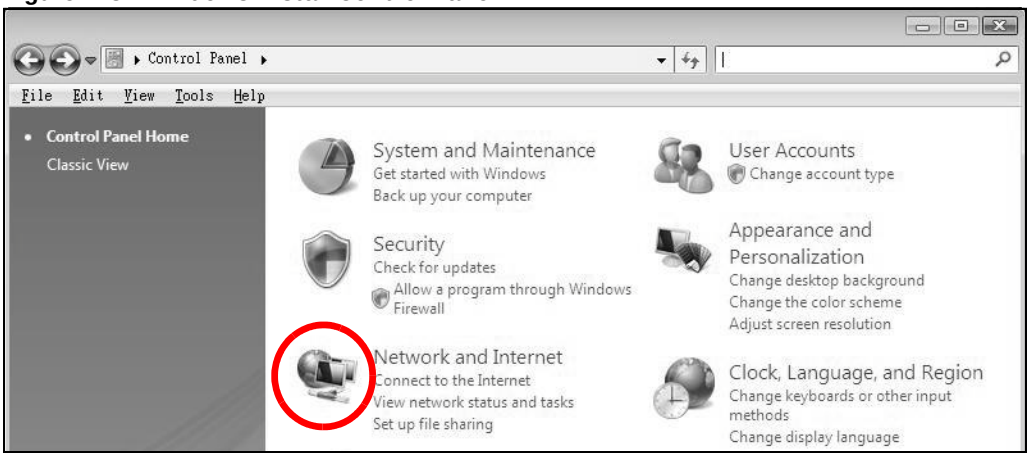
1 Click **Start** > **Control Panel**.

Figure 147 Windows Vista: Start Menu



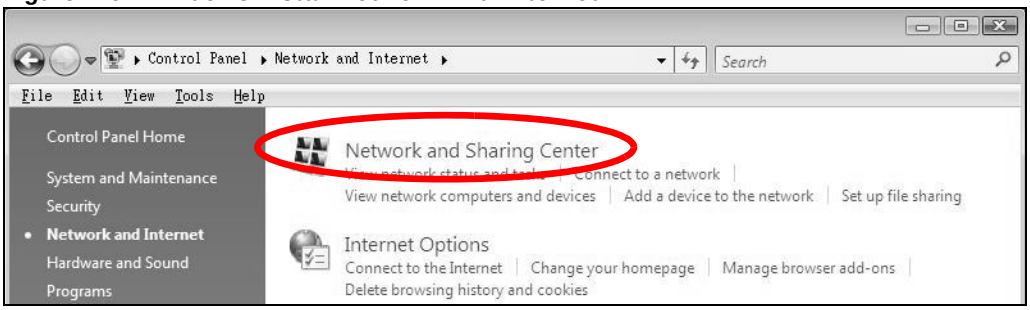
2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 148 Windows Vista: Control Panel



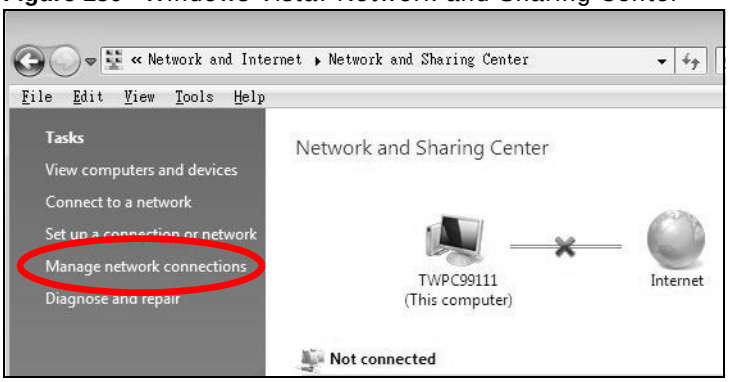
3 Click the **Network and Sharing Center** icon.

Figure 149 Windows Vista: Network And Internet



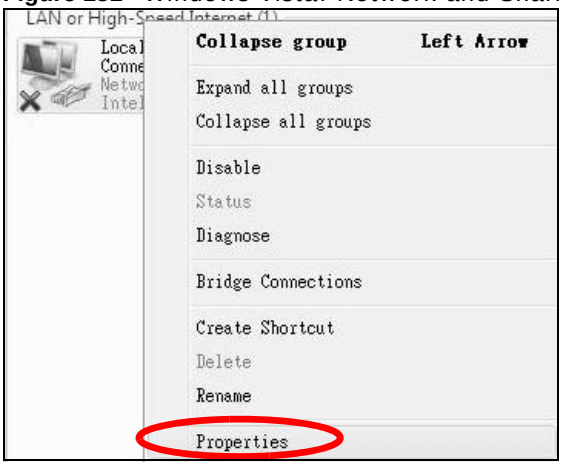
4 Click **Manage network connections**.

Figure 150 Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then select **Properties**.

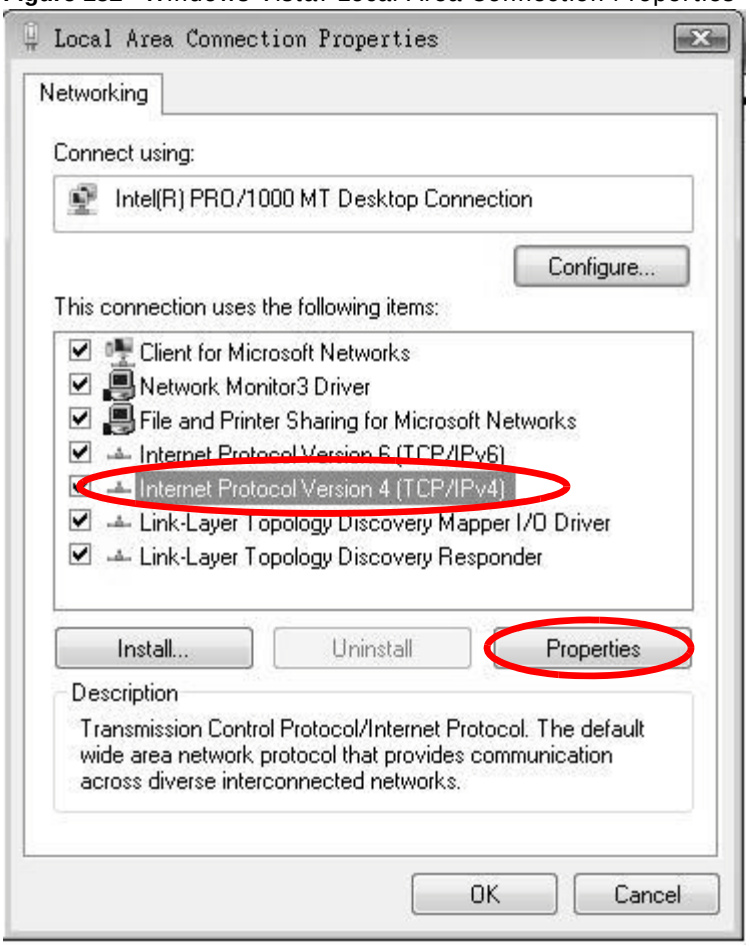
Figure 151 Windows Vista: Network and Sharing Center



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 152 Windows Vista: Local Area Connection Properties



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 153 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

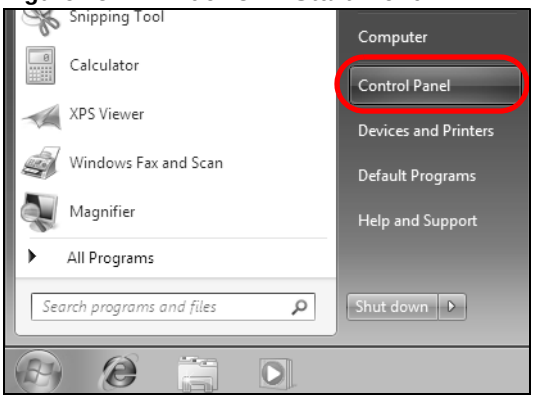
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows 7

This section shows screens from Windows 7 Enterprise.

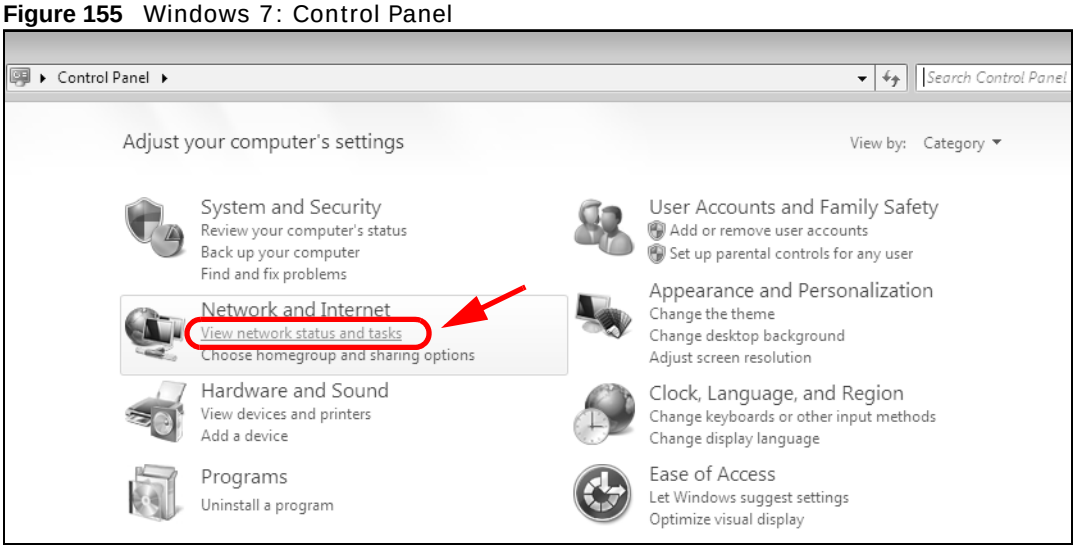
1 Click **Start** > **Control Panel**.

Figure 154 Windows 7: Start Menu



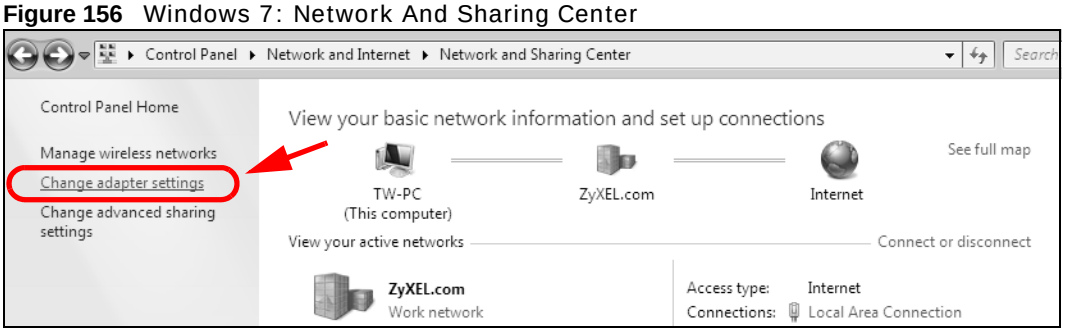
2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

Figure 155 Windows 7: Control Panel



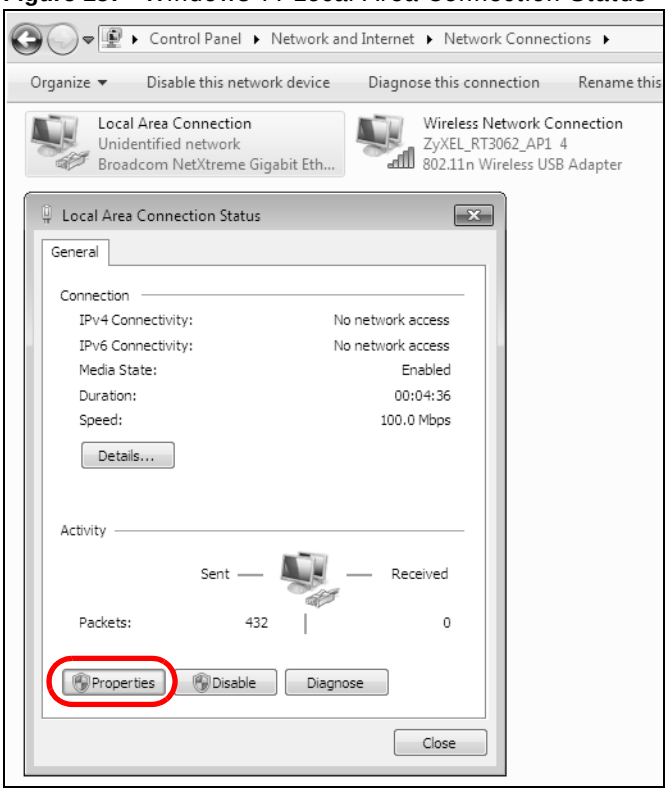
3 Click **Change adapter settings**.

Figure 156 Windows 7: Network And Sharing Center



4 Double click **Local Area Connection** and then select **Properties**.

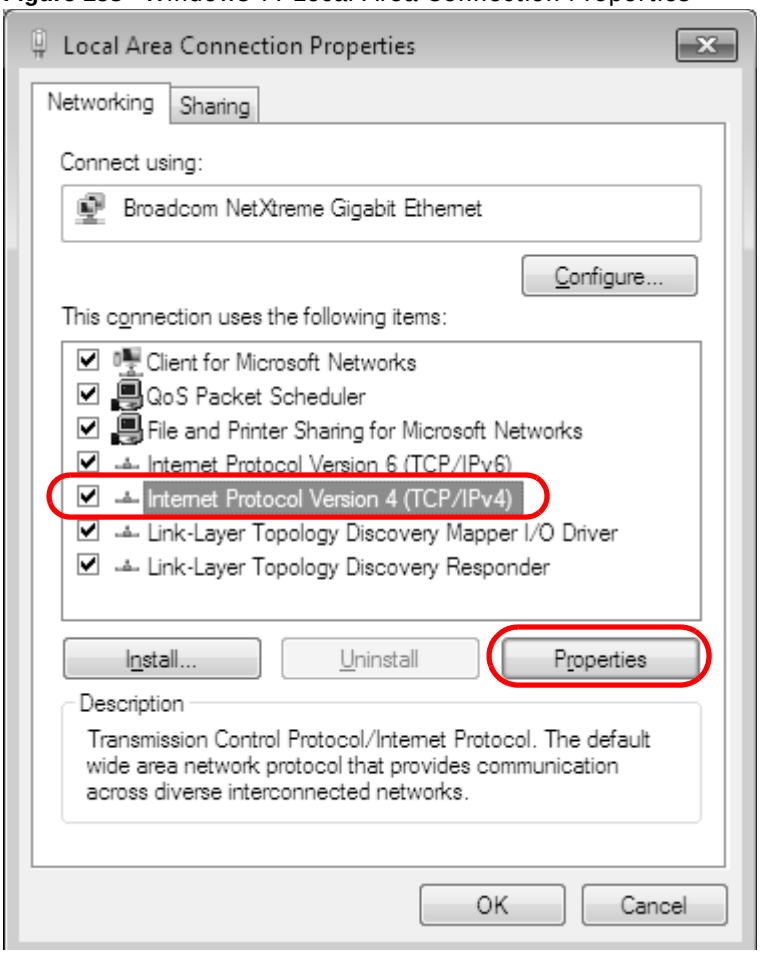
Figure 157 Windows 7: Local Area Connection Status



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

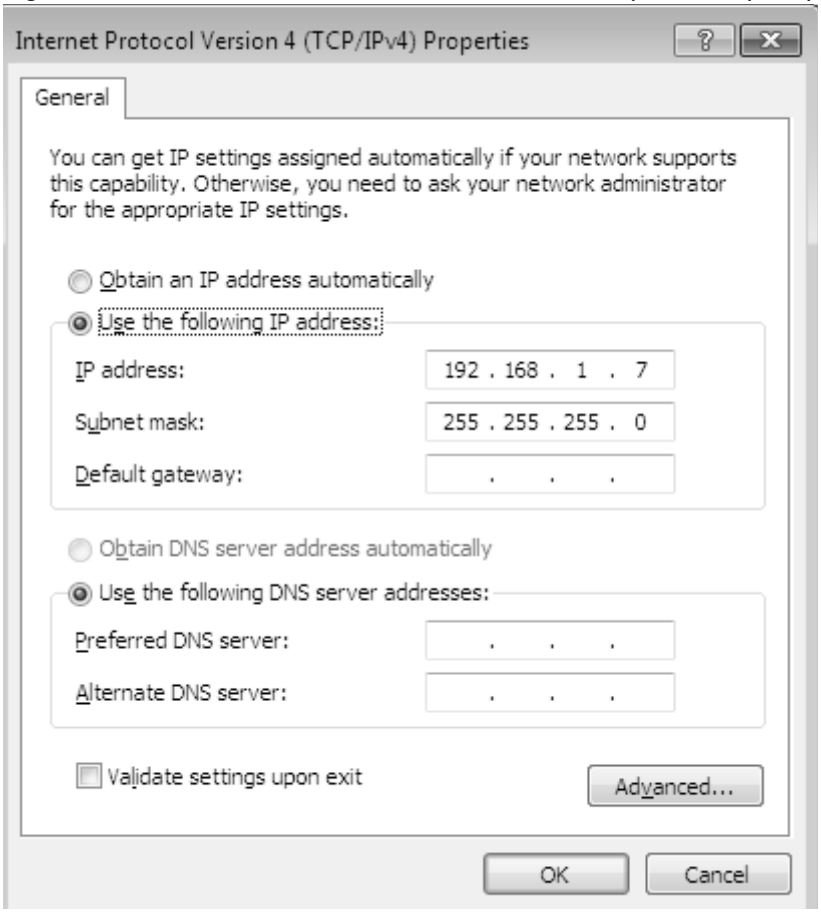
5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 158 Windows 7: Local Area Connection Properties



6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 159 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 1 . 7
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

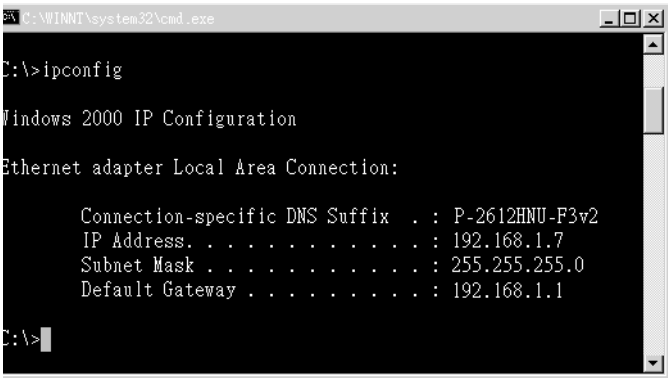
Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

3 The IP settings are displayed as follows.

Figure 160 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties


C:\WINNT\system32\cmd.exe
C:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : P-2612HNU-F3v2
IP Address. . . . . : 192.168.1.7
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
C:\>

Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

Figure 161 Mac OS X 10.4: Apple Menu



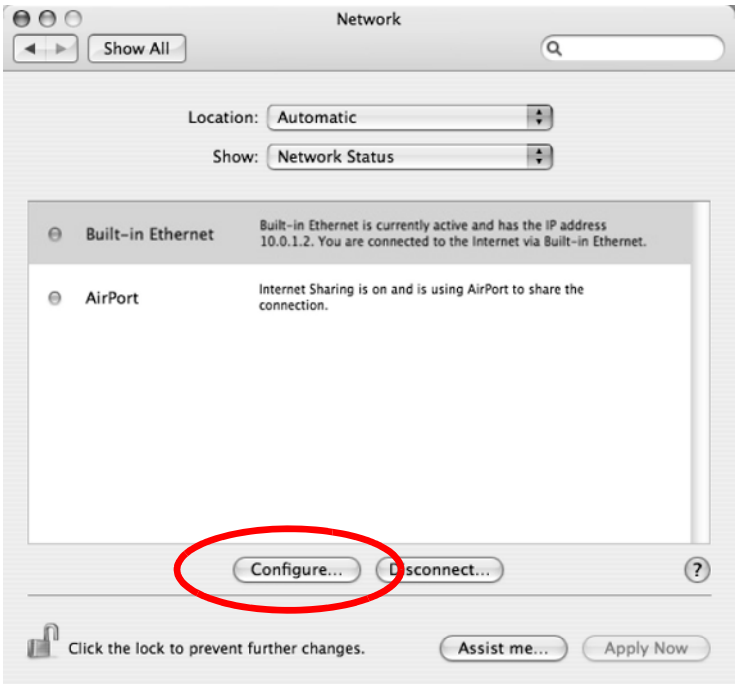
2 In the **System Preferences** window, click the **Network** icon.

Figure 162 Mac OS X 10.4: System Preferences



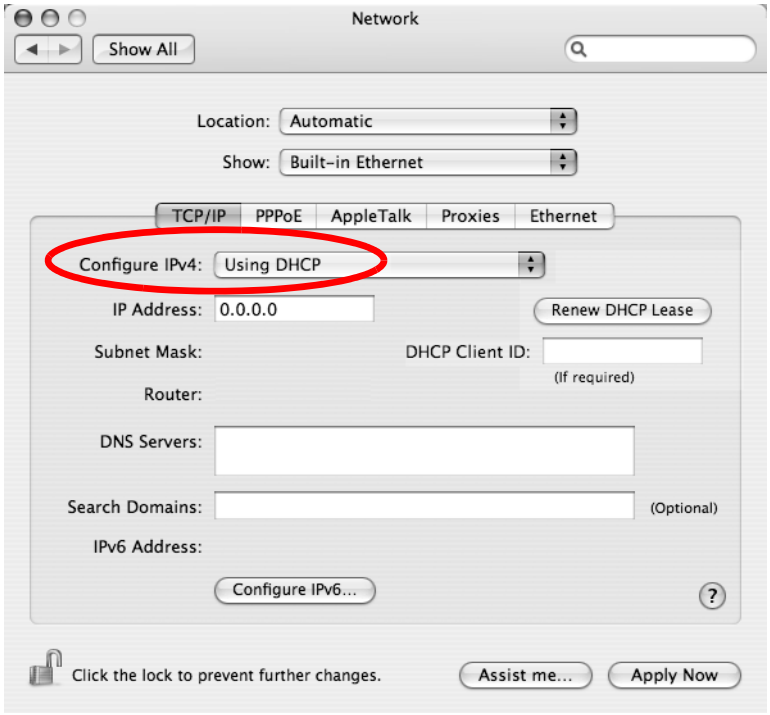
3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

Figure 163 Mac OS X 10.4: Network Preferences


Network
Show All
Location: Automatic
Show: Network Status
Built-in Ethernet
Built-in Ethernet is currently active and has the IP address 10.0.1.2. You are connected to the Internet via Built-in Ethernet.
AirPort
Internet Sharing is on and is using AirPort to share the connection.
Configure...
Disconnect...
Click the lock to prevent further changes.
Assist me...
Apply Now

4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

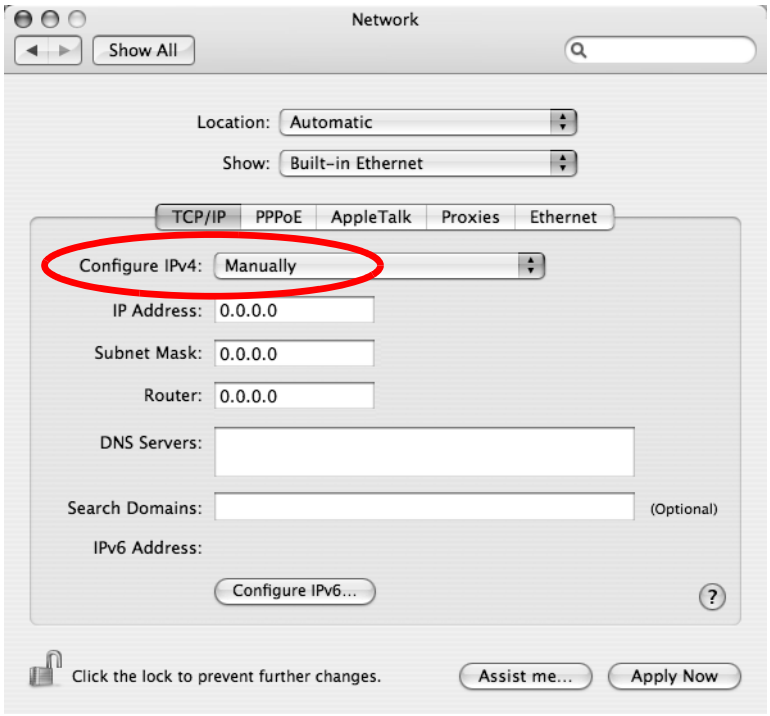
Figure 164 Mac OS X 10.4: Network Preferences > TCP/IP Tab.



5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.
- In the **Router** field, type the IP address of your device.

Figure 165 Mac OS X 10.4: Network Preferences > Ethernet

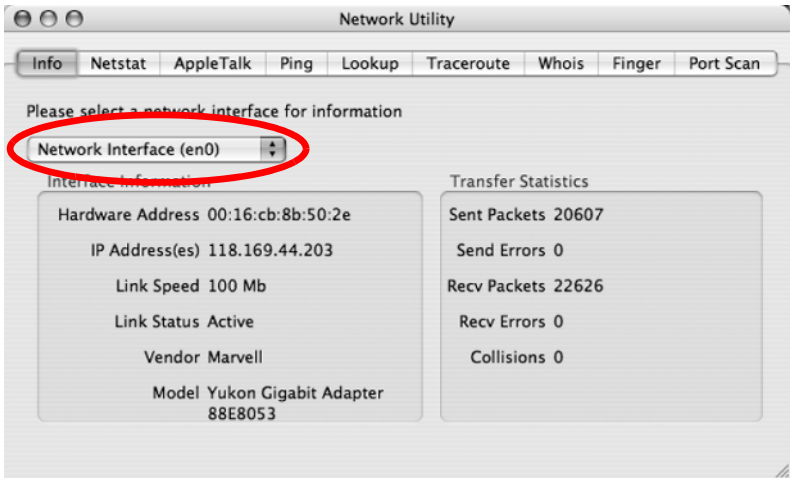


6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 166 Mac OS X 10.4: Network Utility

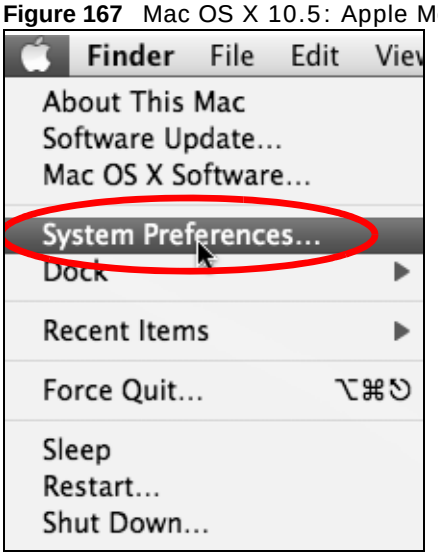


Mac OS X: 10.5

The screens in this section are from Mac OS X 10.5.

1 Click **Apple** > **System Preferences**.

Figure 167 Mac OS X 10.5: Apple Menu



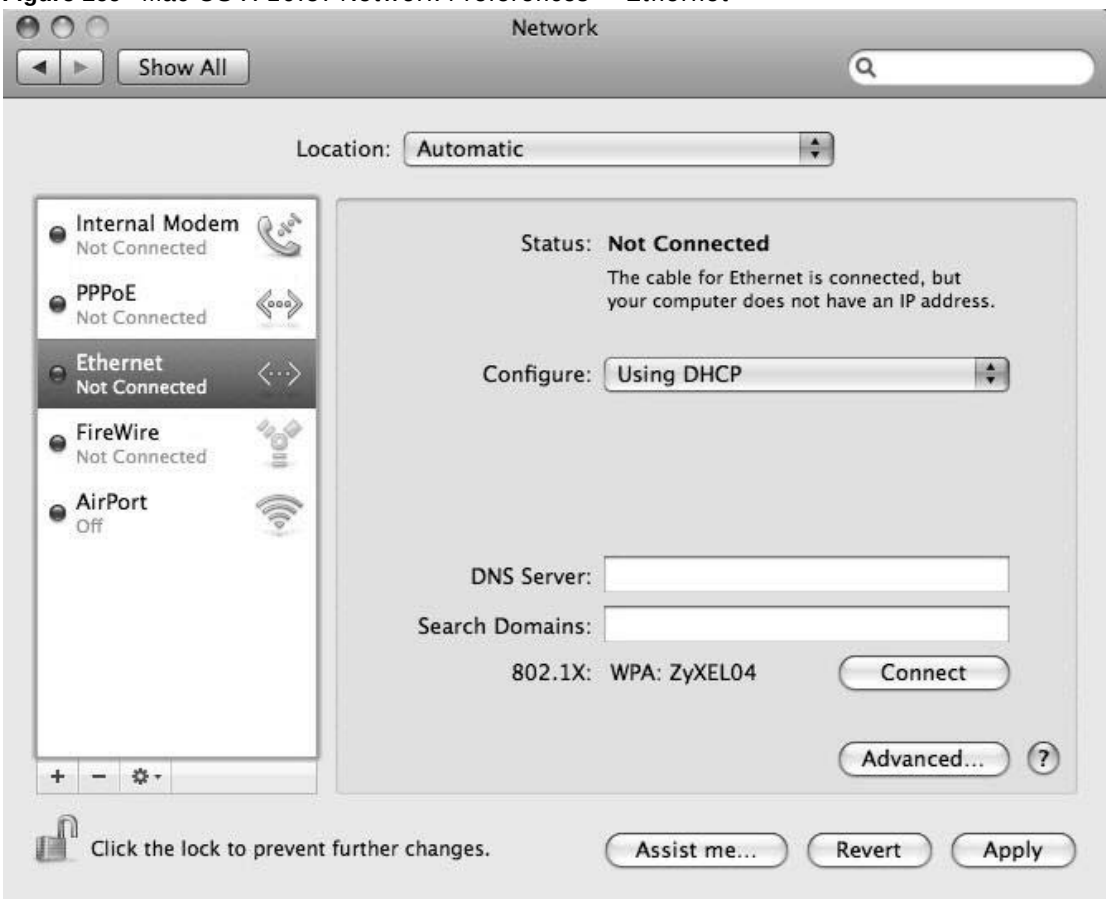
2 In **System Preferences**, click the **Network** icon.

Figure 168 Mac OS X 10.5: Systems Preferences



3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

Figure 169 Mac OS X 10.5: Network Preferences > Ethernet

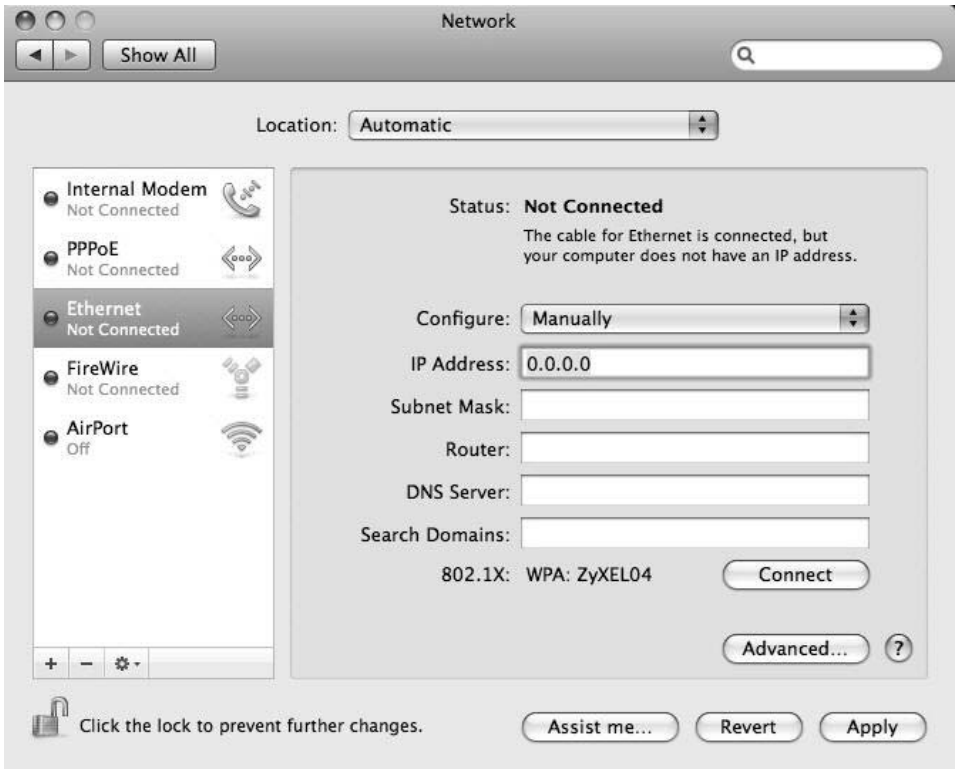


4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.
- In the **Router** field, enter the IP address of your ZyXEL Device.

Figure 170 Mac OS X 10.5: Network Preferences > Ethernet

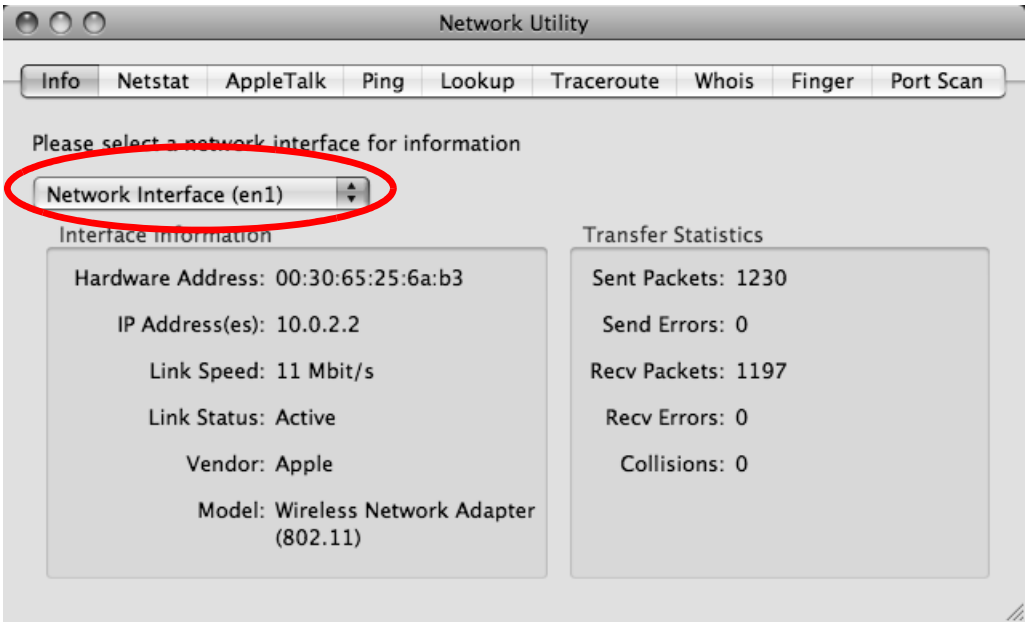


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 171 Mac OS X 10.5: Network Utility



Linux: Ubuntu 8 (GNOME)

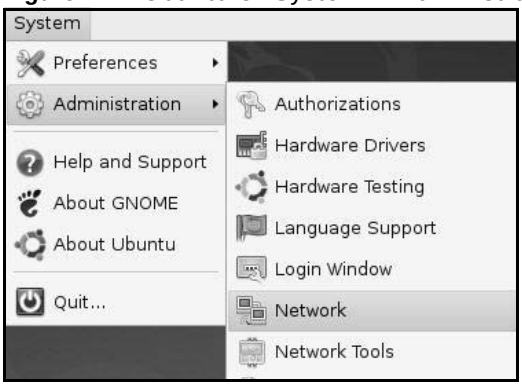
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

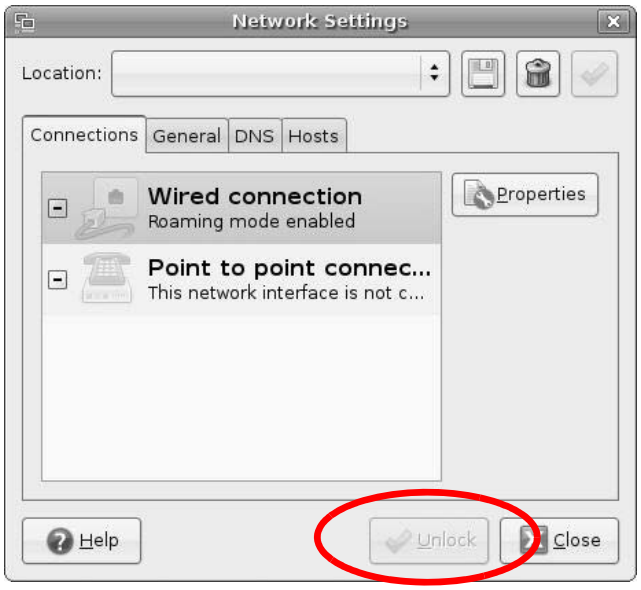
1 Click **System > Administration > Network**.

Figure 172 Ubuntu 8: System > Administration Menu



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 173 Ubuntu 8: Network Settings > Connections



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Figure 174 Ubuntu 8: Administrator Account Authentication


Authenticate
System policy prevents modifying the configuration
An application is attempting to perform an action that requires privileges. Authentication as one of the users below is required to perform this action.
C.J.,,,, (chris)
Password for chris:
Details
Cancel
Authenticate

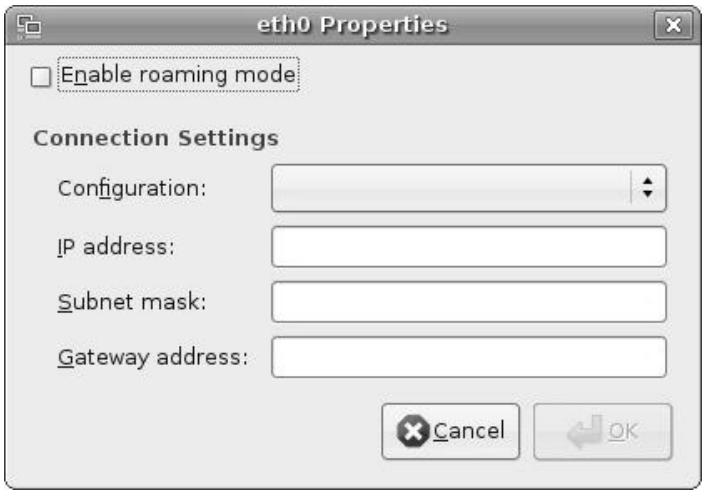
4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 175 Ubuntu 8: Network Settings > Connections



5 The **Properties** dialog box opens.

Figure 176 Ubuntu 8: Network Settings > Properties

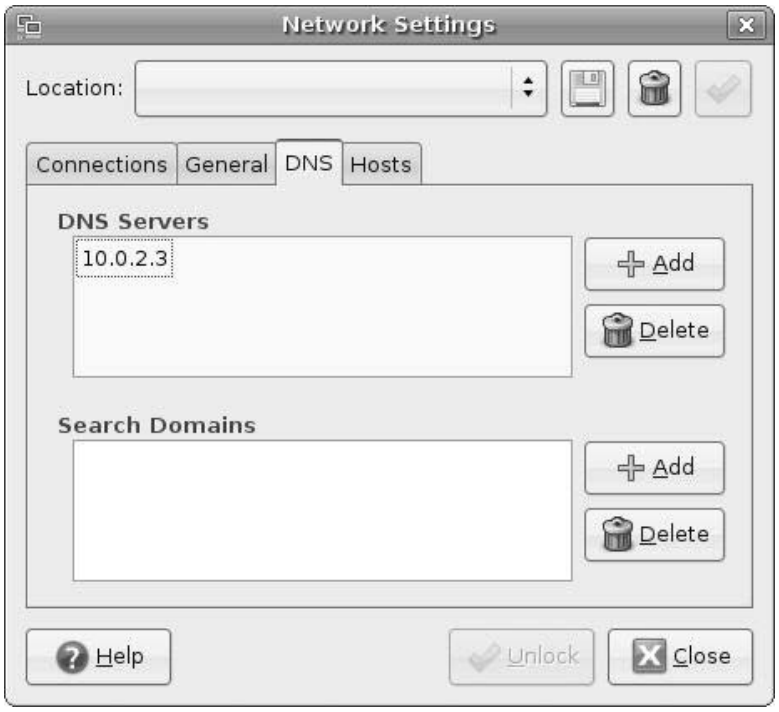


- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

Figure 177 Ubuntu 8: Network Settings > DNS

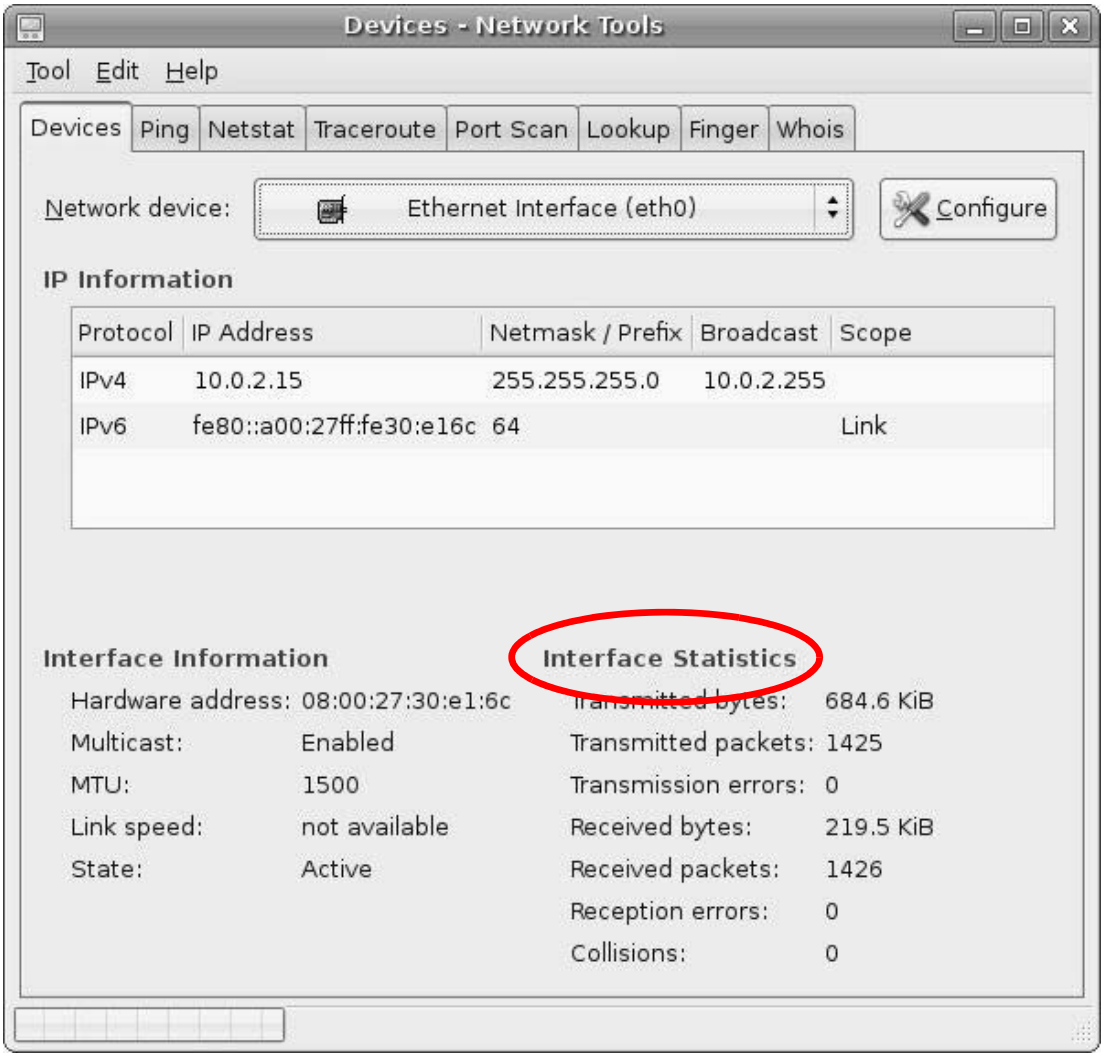


8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices** tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 178 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

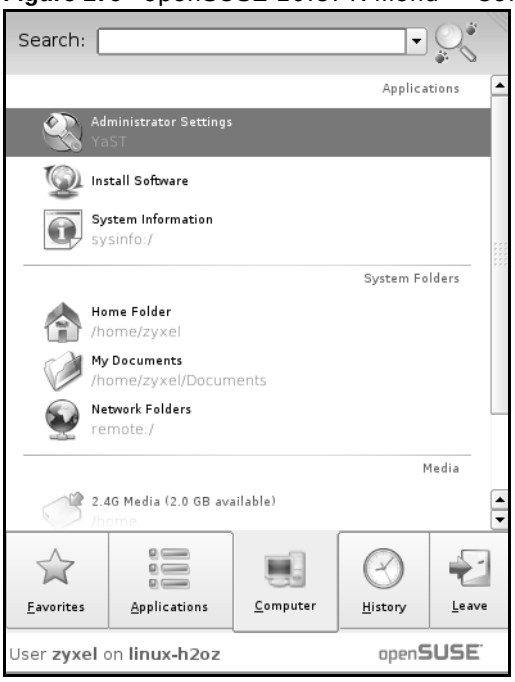
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

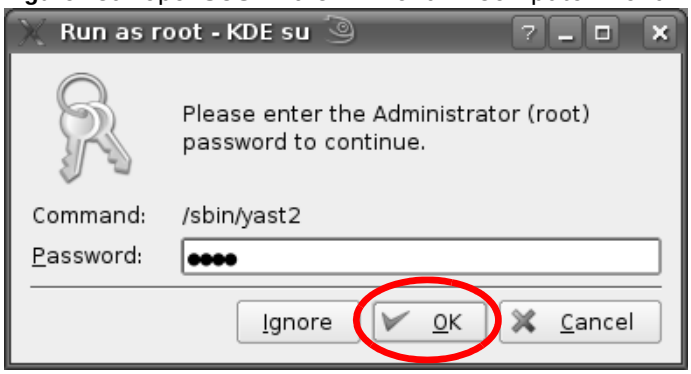
1 Click **K Menu > Computer > Administrator Settings (YaST)**.

Figure 179 openSUSE 10.3: K Menu > Computer Menu



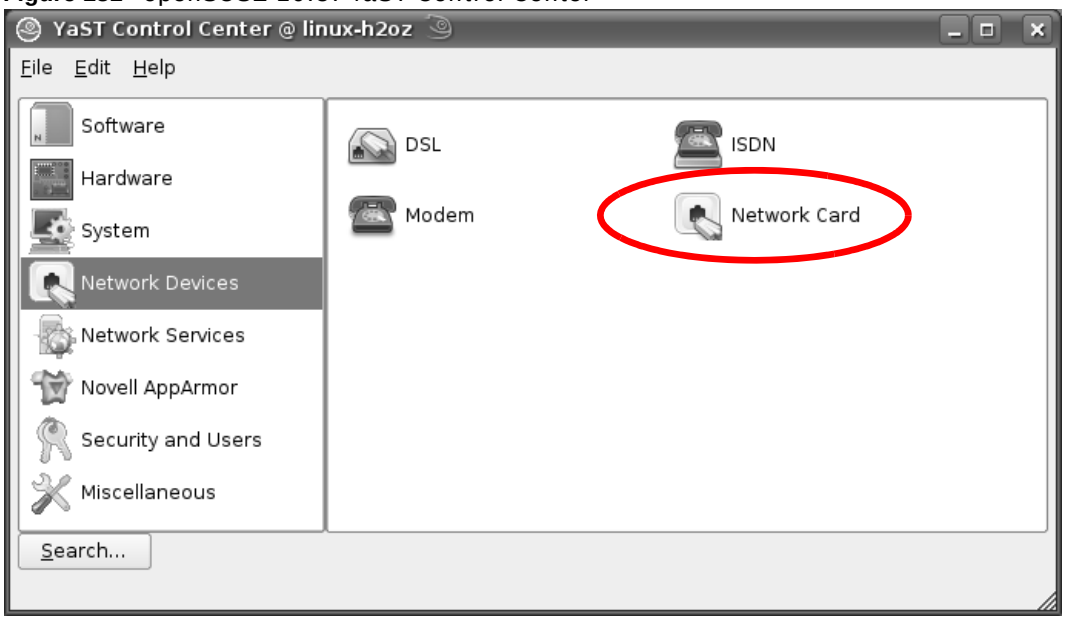
2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 180 openSUSE 10.3: K Menu > Computer Menu



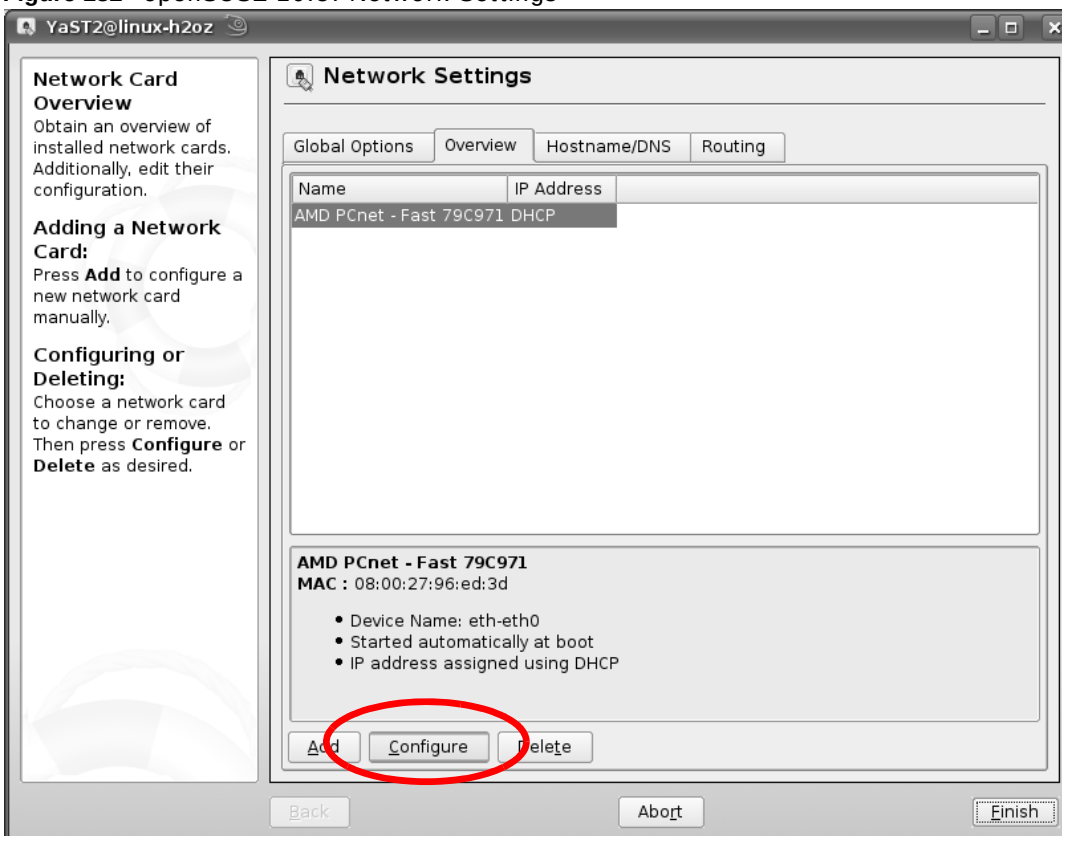
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 181 openSUSE 10.3: YaST Control Center



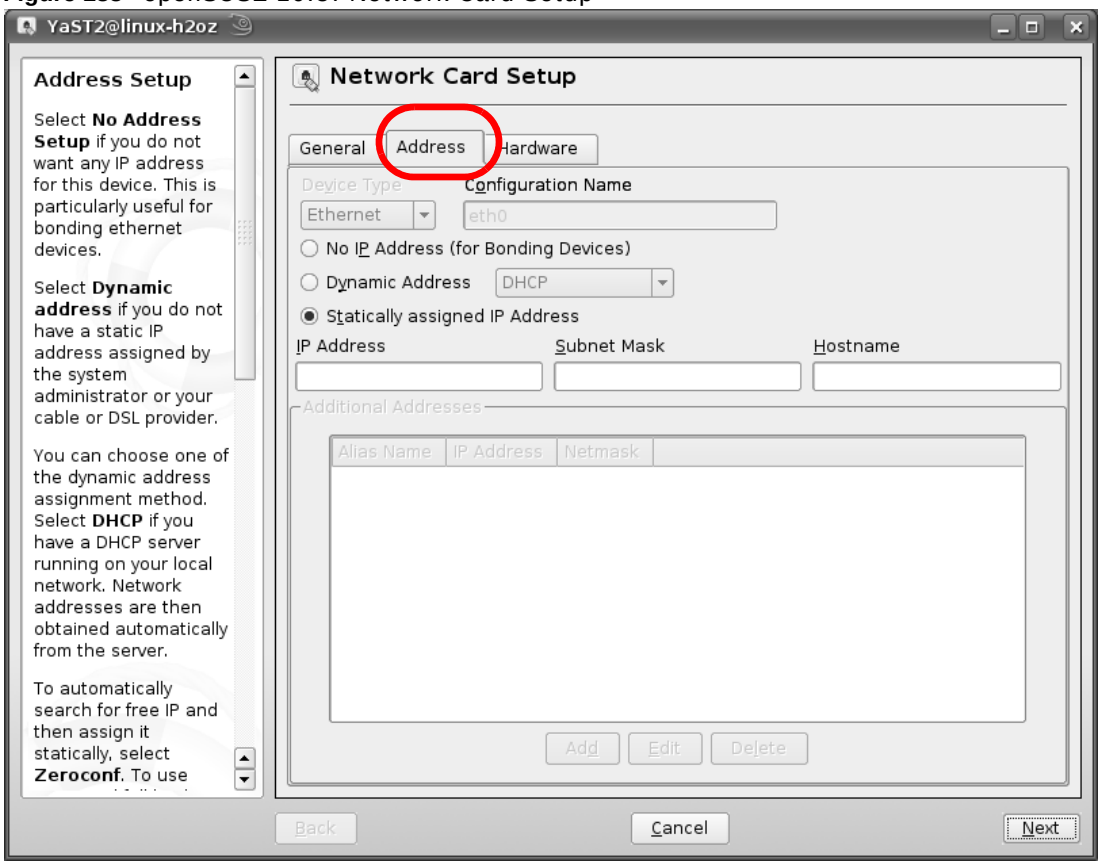
4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 182 openSUSE 10.3: Network Settings



5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 183 openSUSE 10.3: Network Card Setup


YaST2@linux-h2oz
Address Setup
Select No Address Setup if you do not want any IP address for this device. This is particularly useful for bonding ethernet devices.
Select Dynamic address if you do not have a static IP address assigned by the system administrator or your cable or DSL provider.
You can choose one of the dynamic address assignment method. Select DHCP if you have a DHCP server running on your local network. Network addresses are then obtained automatically from the server.
To automatically search for free IP and then assign it statically, select Zeroconf. To use
Network Card Setup
General
Address
Hardware
Device Type
Configuration Name
Ethernet
eth0
No IP Address (for Bonding Devices)
Dynamic Address
DHCP
Statically assigned IP Address
IP Address
Subnet Mask
Hostname
Additional Addresses
Alias Name
IP Address
Netmask
Add
Edit
Delete
Back
Cancel
Next

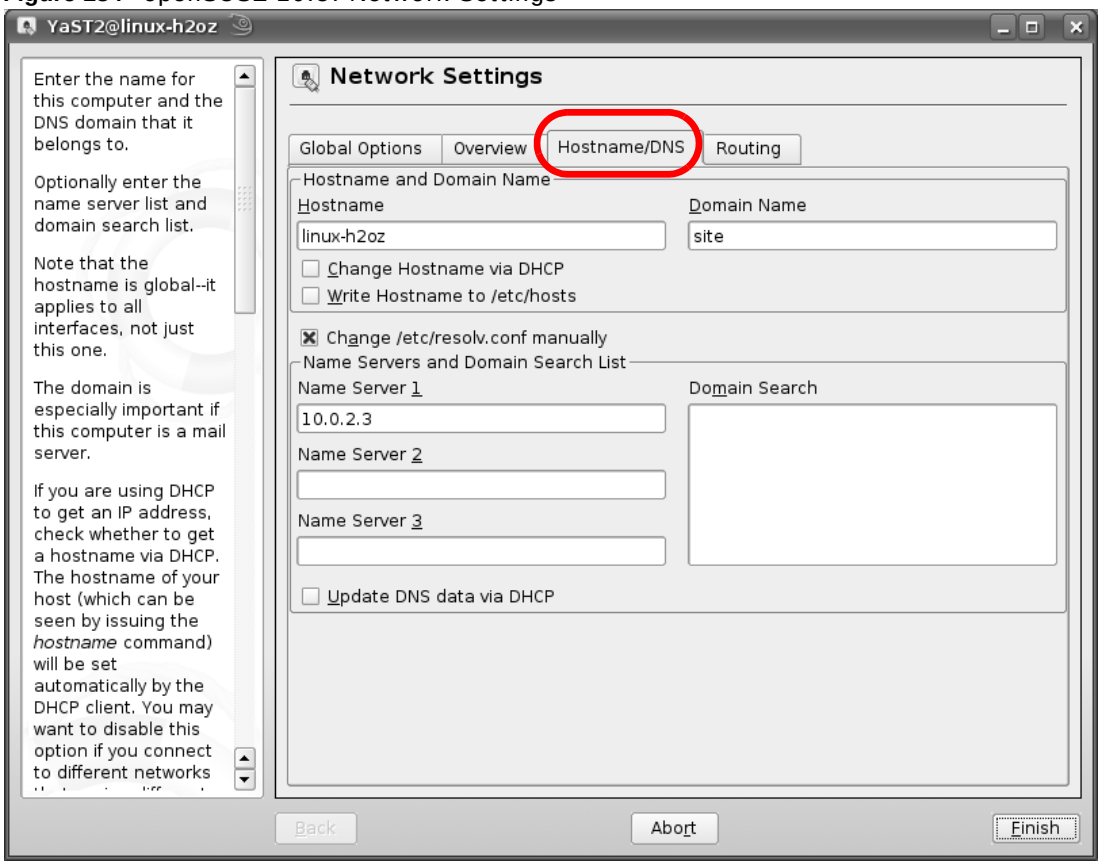
6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname / DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

Figure 184 openSUSE 10.3: Network Settings

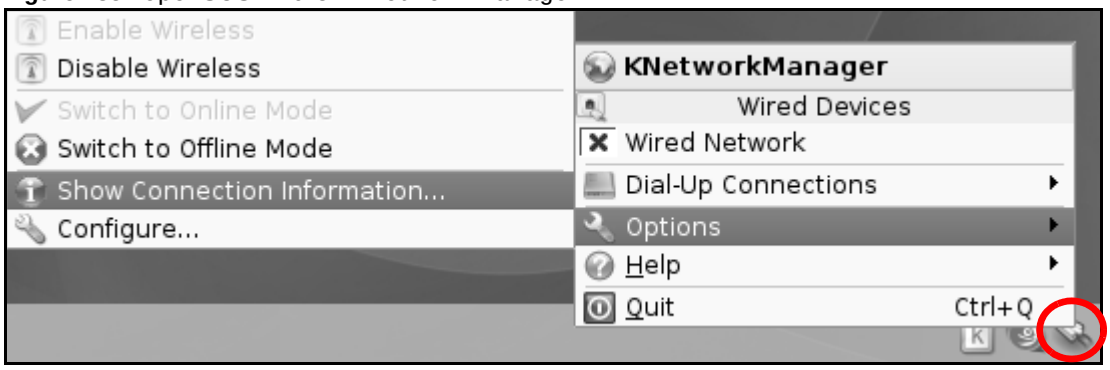

YaST2@linux-h2oz
Enter the name for this computer and the DNS domain that it belongs to.
Optionally enter the name server list and domain search list.
Note that the hostname is global--it applies to all interfaces, not just this one.
The domain is especially important if this computer is a mail server.
If you are using DHCP to get an IP address, check whether to get a hostname via DHCP. The hostname of your host (which can be seen by issuing the hostname command) will be set automatically by the DHCP client. You may want to disable this option if you connect to different networks
Network Settings
Global Options
Overview
Hostname/DNS
Routing
Hostname and Domain Name
Hostname
linux-h2oz
Domain Name
site
Change Hostname via DHCP
Write Hostname to /etc/hosts
Change /etc/resolv.conf manually
Name Servers and Domain Search List
Name Server 1
10.0.2.3
Domain Search
Name Server 2
Name Server 3
Update DNS data via DHCP
Back
Abort
Finish

9 Click **Finish** to save your settings and close the window.

Verifying Settings

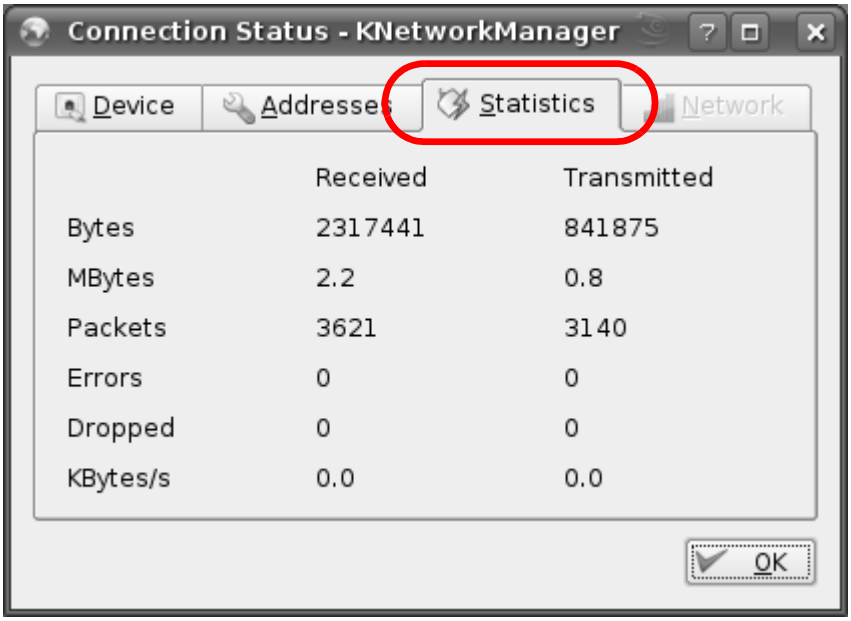
Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 185 openSUSE 10.3: KNetwork Manager



When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 186 openSUSE: Connection Status - KNetwork Manager



C

Pop-up Windows, Java Script and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

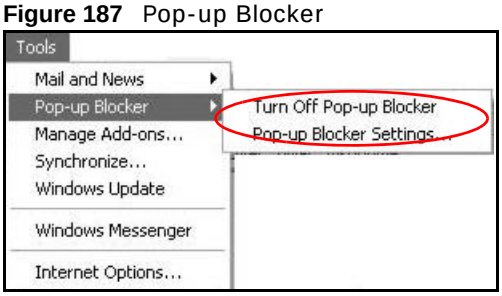
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 187 Pop-up Blocker

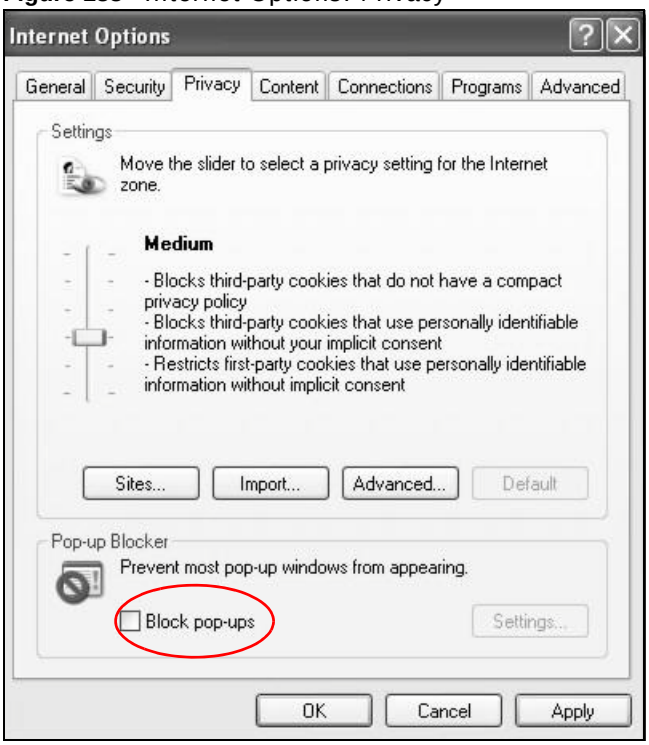


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 188 Internet Options: Privacy



3 Click **Apply** to save this setting.

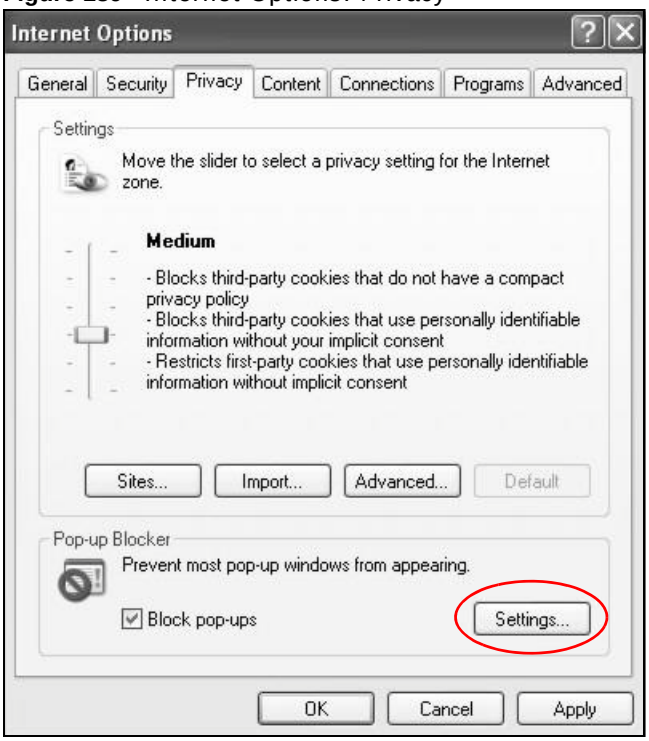
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

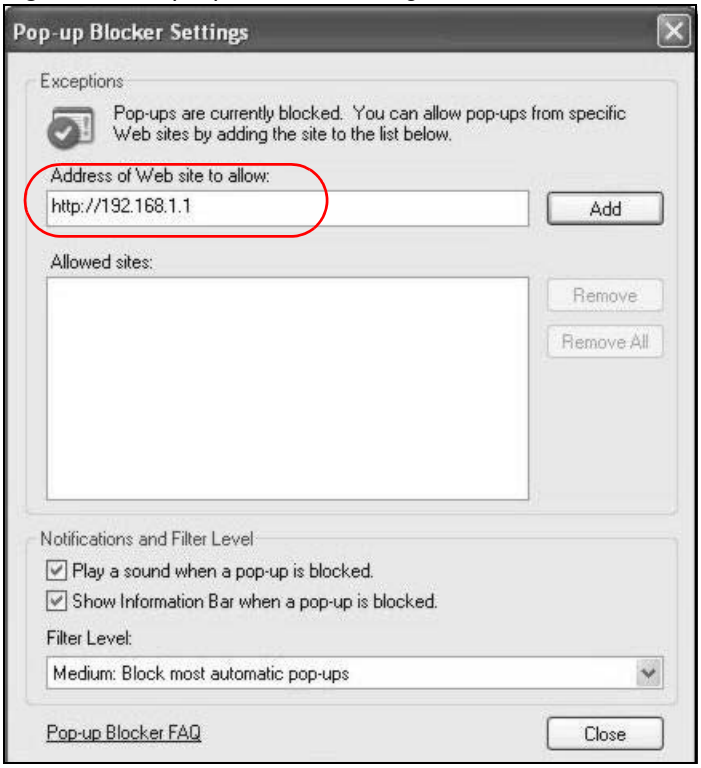
Figure 189 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 190 Pop-up Blocker Settings


Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

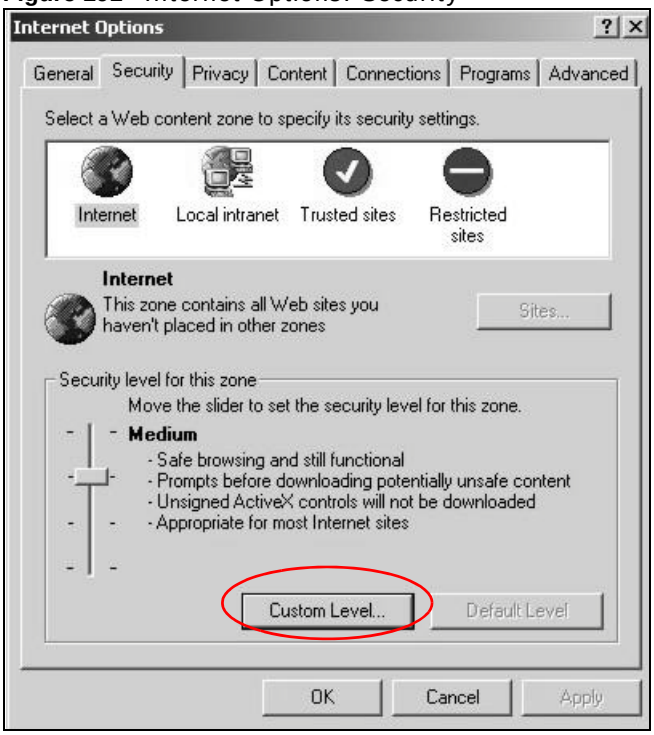
6 Click **Apply** to save this setting.

JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 191 Internet Options: Security



2 Click the **Custom Level...** button.

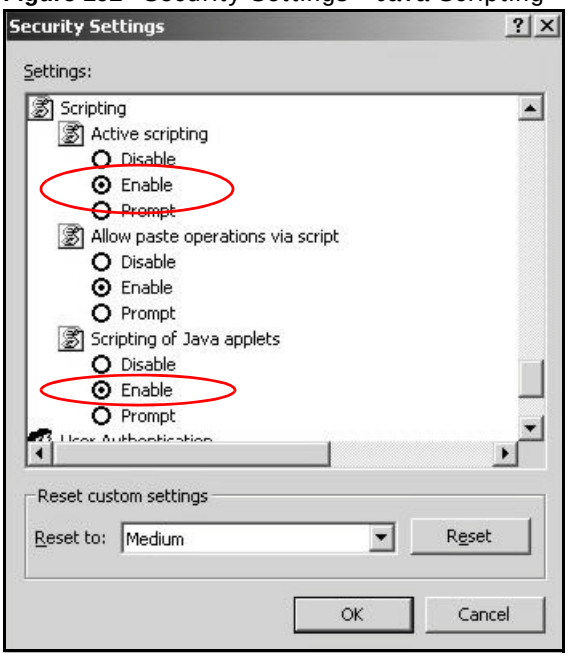
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 192 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

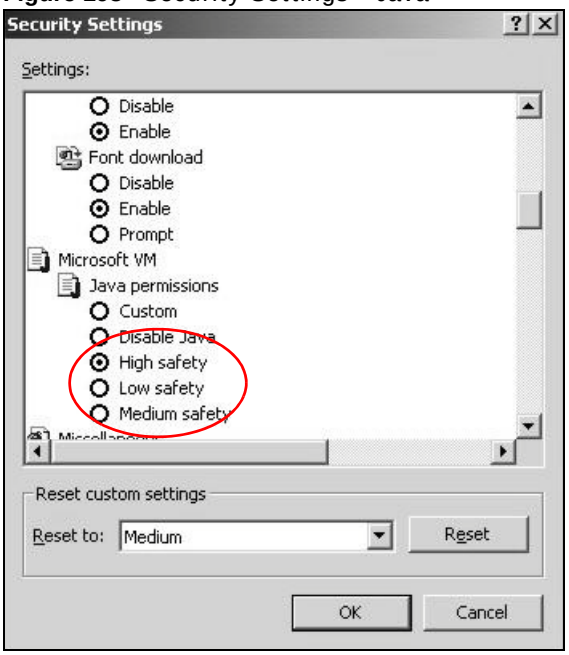
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 193 Security Settings - Java



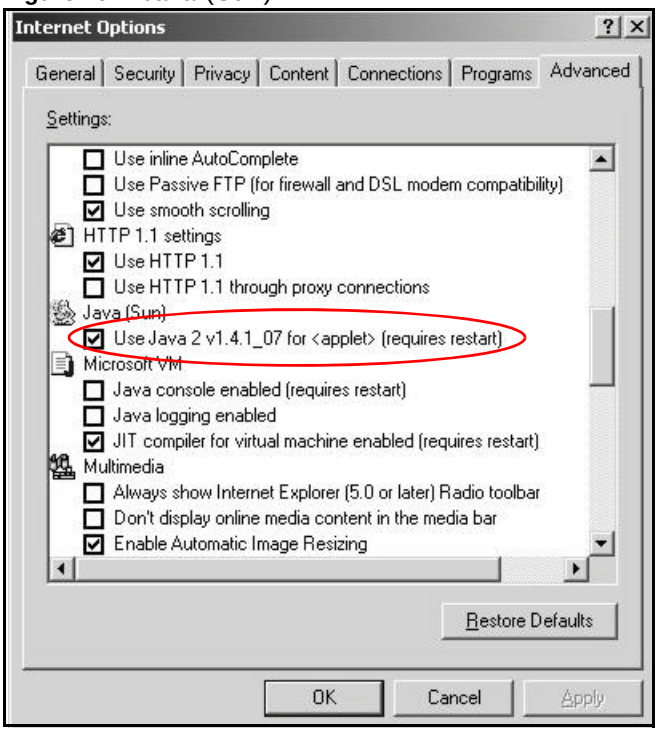
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 194 Java (Sun)



Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

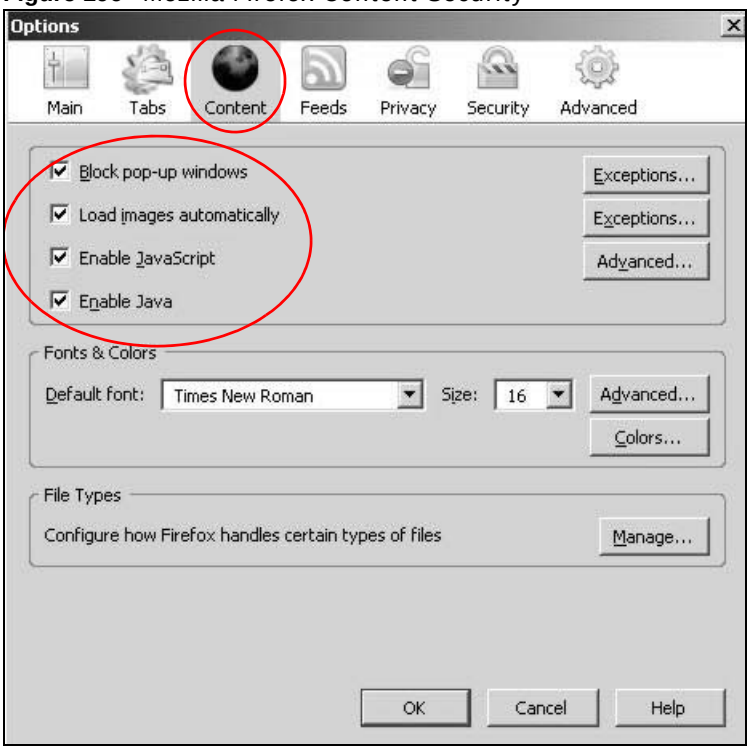
You can enable Java, JavaScript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 195 Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 196 Mozilla Firefox Content Security



D

Wireless LANs

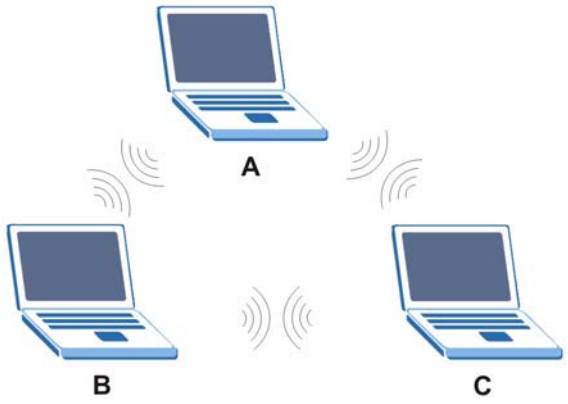
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 197 Peer-to-Peer Communication in an Ad-hoc Network

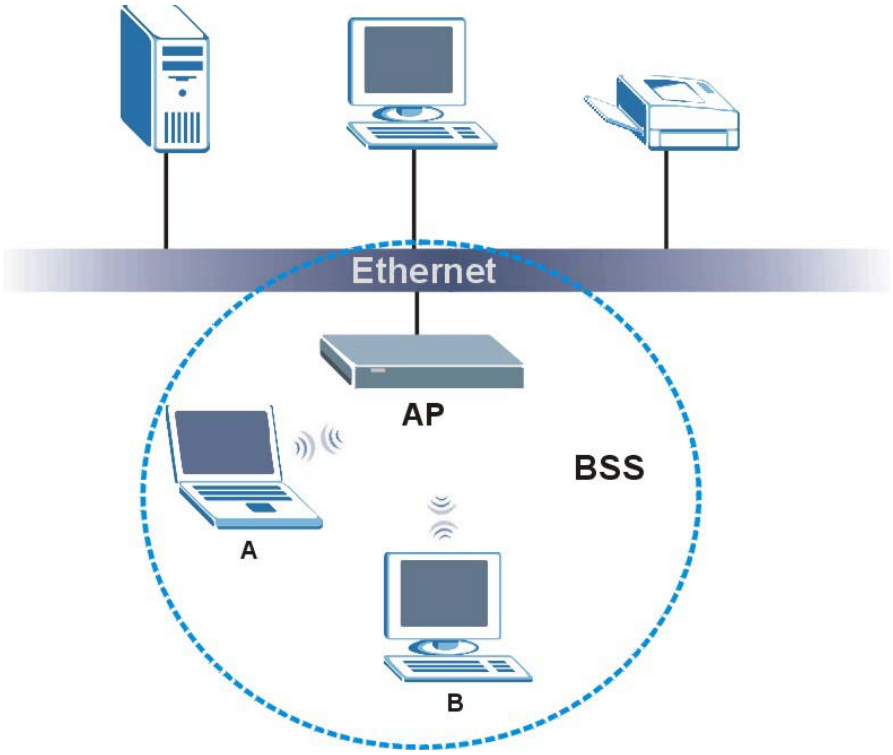


BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 198 Basic Service Set



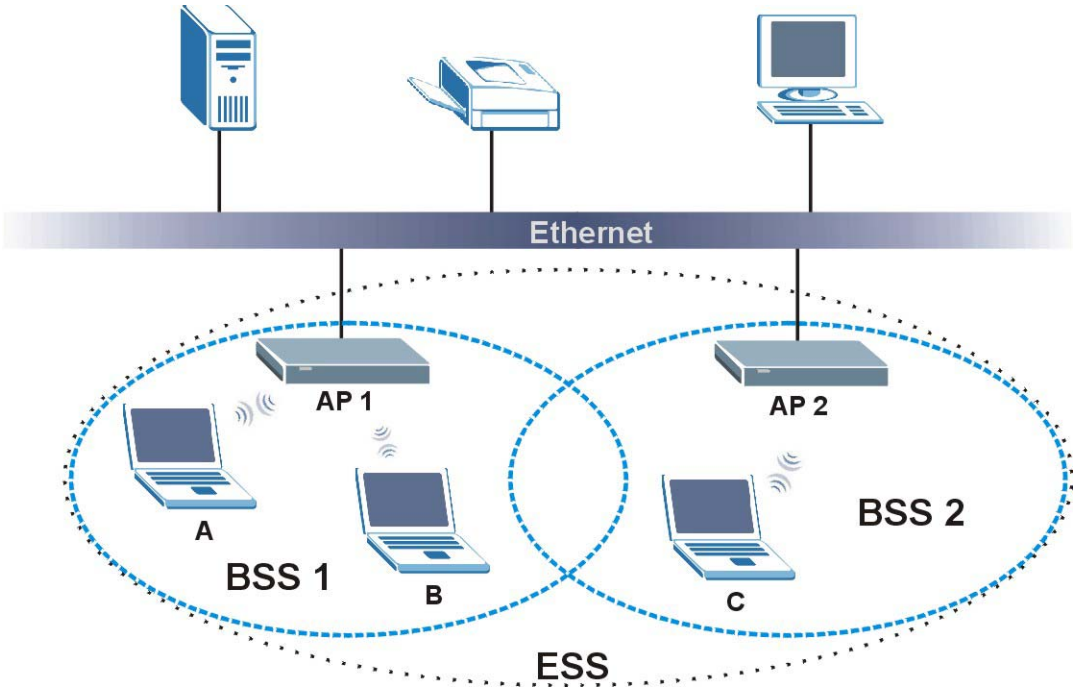
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 199 Infrastructure WLAN



Channel

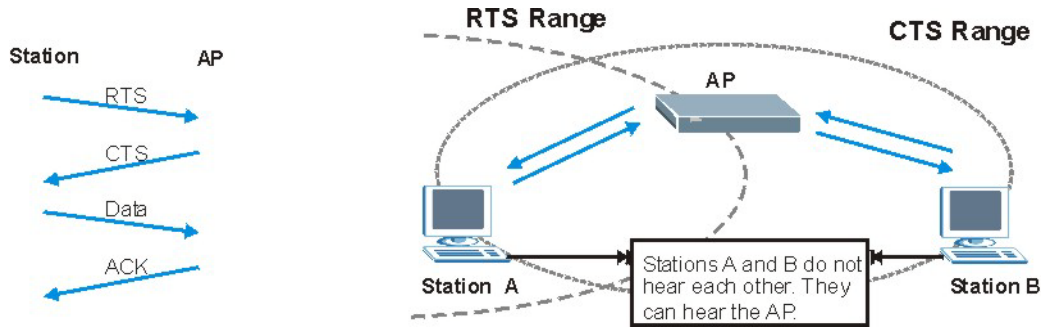
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 200 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the ZyXEL Device uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 102 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the ZyXEL Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyXEL Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your ZyXEL Device.

Table 103 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
	WPA2
Most Secure	

Note: You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 104 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm

called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

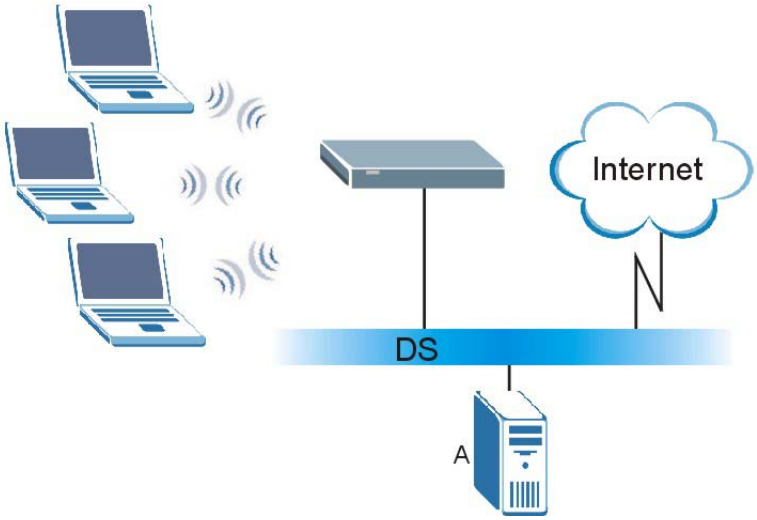
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4. The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 201 WPA(2) with RADIUS Application Example



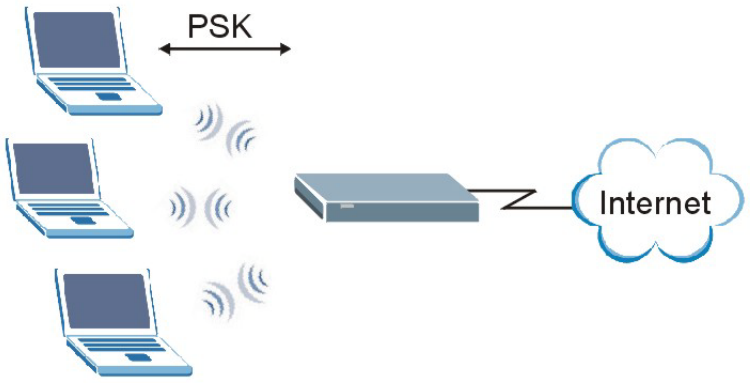
WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each wireless client's password and allows it to join the network only if the password matches.
3. The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 202 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 105 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

WiFi Protected Setup

Your ZyXEL Device supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

Push Button Configuration

WPS Push Button Configuration (PBC) is initiated by pressing a button on each WPS-enabled device, and allowing them to connect automatically. You do not need to enter any information.

Not every WPS-enabled device has a physical WPS button. Some may have a WPS PBC button in their configuration utilities instead of or in addition to the physical button.

Take the following steps to set up WPS using the button.

1. Ensure that the two devices you want to set up are within wireless range of one another.
2. Look for a WPS button on each device. If the device does not have one, log into its configuration utility and locate the button (see the device's User's Guide for how to do this - for the ZyXEL Device, see Section 6.4 on page 115).
3. Press the button on one of the devices (it doesn't matter which).
4. Within two minutes, press the button on the other device. The registrar sends the network name (SSID) and security key through an secure connection to the enrollee.

   If you need to make sure that WPS worked, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

PIN Configuration

Each WPS-enabled device has its own PIN (Personal Identification Number). This may either be static (it cannot be changed) or dynamic (you can change it to a new random number by clicking on a button in the configuration interface).

When you use the PIN method, you must enter the enrollee's PIN into the registrar. Then, when WPS is activated on the enrollee, it presents its PIN to the registrar. If the PIN matches, the registrar sends the network and security information to the enrollee, allowing it to join the network.

The advantage of using the PIN method rather than the PBC method is that you can ensure that the connection is established between the devices you specify, not just the first two devices to activate WPS in the area. However, you need to log into the configuration interfaces of both devices.

Take the following steps to set up WPS using the PIN method.

1 Decide which device you want to be the registrar (usually the AP) and which you want to be the enrollee (usually the client).

2 Look for the enrollee's WPS PIN; it may be displayed on the device. If you don't see it, log into the enrollee's configuration interface and locate the PIN. Select the PIN connection mode (not PBC connection mode). See the device's User's Guide for how to do this - for the ZyXEL Device, see Section 6.4 on page 115.

3 Log into the configuration utility of the registrar. Select the PIN connection mode (not the PBC connection mode). Locate the place where you can enter the enrollee's PIN (if you are using the ZyXEL Device, see Section 6.4 on page 115). Enter the PIN from the enrollee device.

4 Activate WPS on both devices within two minutes.

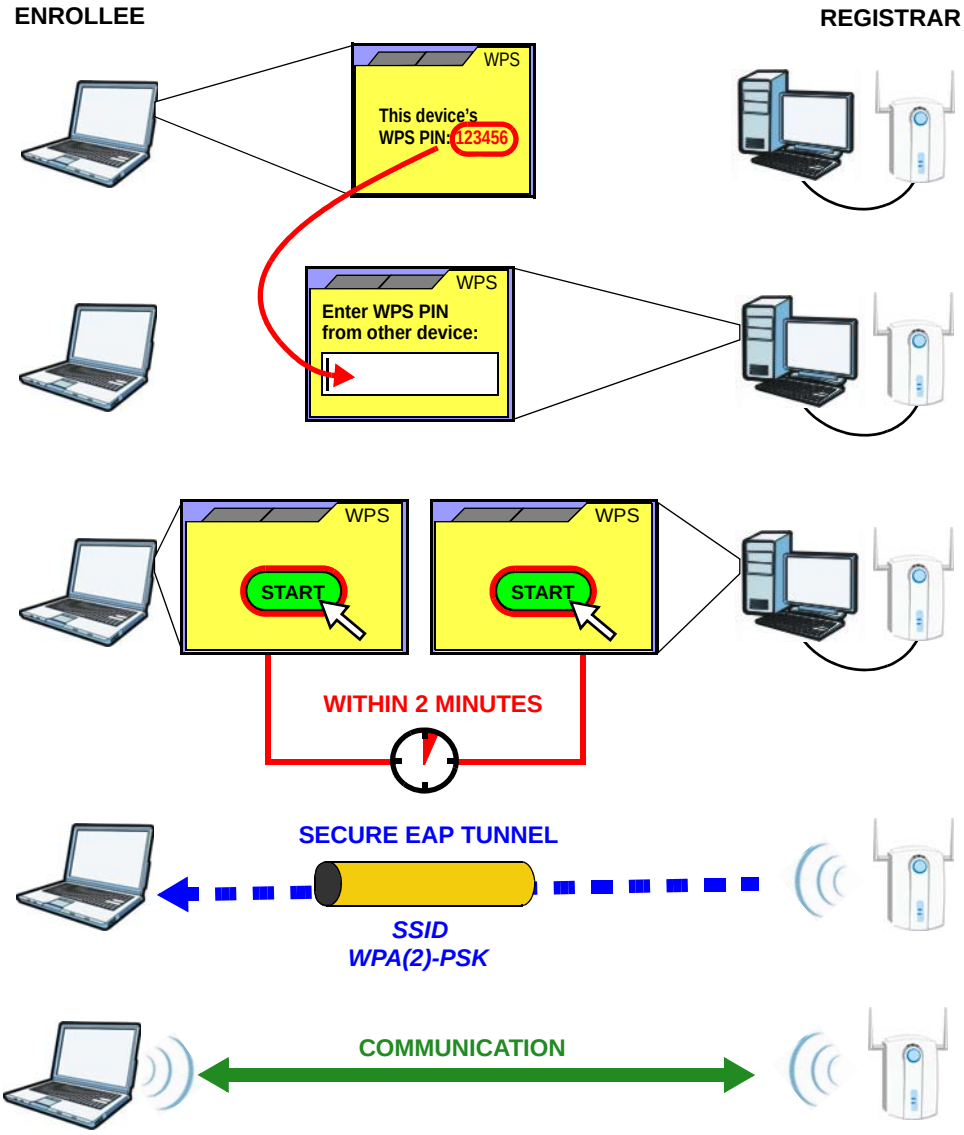
Note: Use the configuration utility to activate WPS, not the push-button on the device itself.

5 On a computer connected to the wireless client, try to connect to the Internet. If you can connect, WPS was successful.

If you cannot connect, check the list of associated wireless clients in the AP's configuration utility. If you see the wireless client in the list, WPS was successful.

The following figure shows a WPS-enabled wireless client (installed in a notebook computer) connecting to the WPS-enabled AP via the PIN method.

Figure 203 Example WPS Process: PIN Method

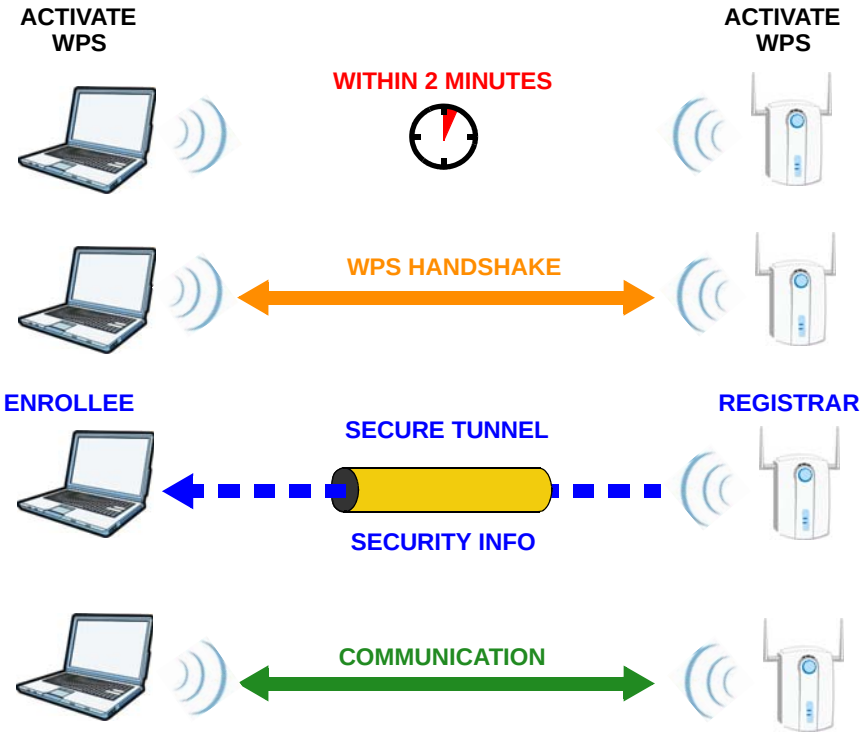


How WPS Works

When two WPS-enabled devices connect, each device must assume a specific role. One device acts as the registrar (the device that supplies network and security settings) and the other device acts as the enrollee (the device that receives network and security settings. The registrar creates a secure EAP (Extensible Authentication Protocol) tunnel and sends the network name (SSID) and the WPA-PSK or WPA2-PSK pre-shared key to the enrollee. Whether WPA-PSK or WPA2-PSK is used depends on the standards supported by the devices. If the registrar is already part of a network, it sends the existing information. If not, it generates the SSID and WPA(2)-PSK randomly.

The following figure shows a WPS-enabled client (installed in a notebook computer) connecting to a WPS-enabled access point.

Figure 204 How WPS works



The roles of registrar and enrollee last only as long as the WPS setup process is active (two minutes). The next time you use WPS, a different device can be the registrar if necessary.

The WPS connection process is like a handshake; only two devices participate in each WPS transaction. If you want to add more devices you should repeat the process with one of the existing networked devices and the new device.

Note that the access point (AP) is not always the registrar, and the wireless client is not always the enrollee. All WPS-certified APs can be a registrar, and so can some WPS-enabled wireless clients.

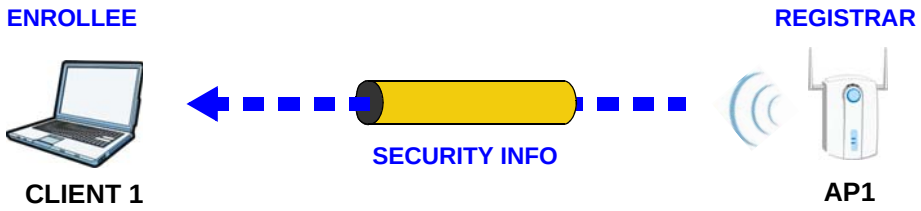
By default, a WPS devices is “unconfigured”. This means that it is not part of an existing network and can act as either enrollee or registrar (if it supports both functions). If the registrar is unconfigured, the security settings it transmits to the enrollee are randomly-generated. Once a WPS-enabled device has connected to another device using WPS, it becomes “configured”. A configured wireless client can still act as enrollee or registrar in subsequent WPS connections, but a configured access point can no longer act as enrollee. It will be the registrar in all subsequent WPS connections in which it is involved. If you want a configured AP to act as an enrollee, you must reset it to its factory defaults.

Example WPS Network Setup

This section shows how security settings are distributed in an example WPS setup.

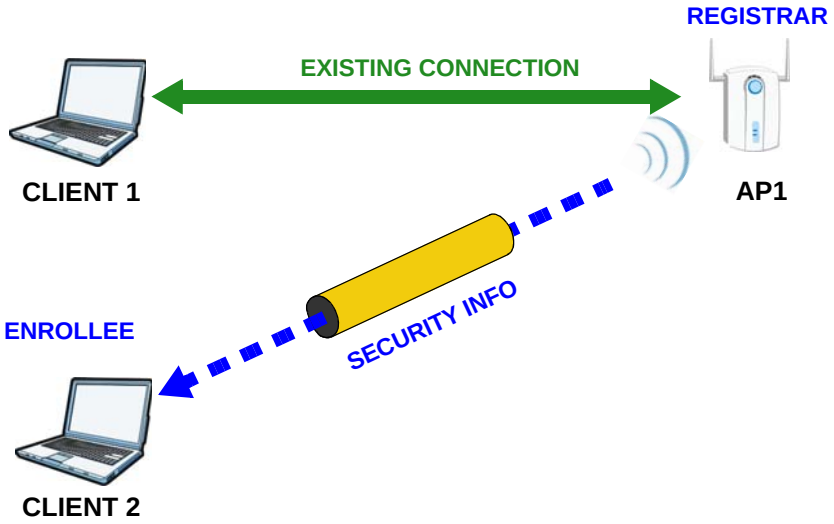
The following figure shows an example network. In step **1**, both **AP1** and **Client 1** are unconfigured. When WPS is activated on both, they perform the handshake. In this example, **AP1** is the registrar, and **Client 1** is the enrollee. The registrar randomly generates the security information to set up the network, since it is unconfigured and has no existing information.

Figure 205 WPS: Example Network Step 1



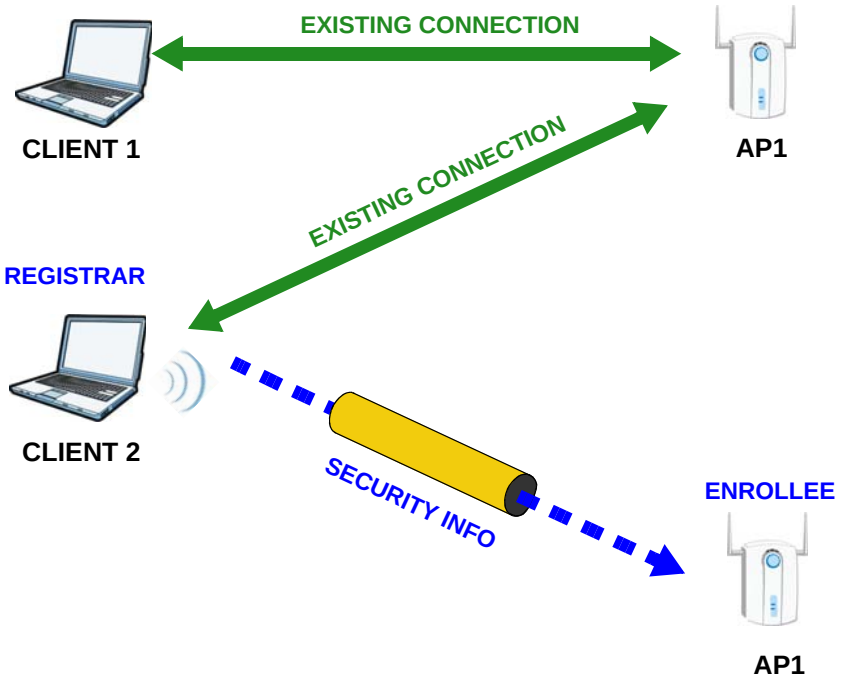
In step **2**, you add another wireless client to the network. You know that **Client 1** supports registrar mode, but it is better to use **AP1** for the WPS handshake with the new client since you must connect to the access point anyway in order to use the network. In this case, **AP1** must be the registrar, since it is configured (it already has security information for the network). **AP1** supplies the existing security information to **Client 2**.

Figure 206 WPS: Example Network Step 2



In step 3, you add another access point (**AP2**) to your network. **AP2** is out of range of **AP1**, so you cannot use **AP1** for the WPS handshake with the new access point. However, you know that **Client 2** supports the registrar function, so you use it to perform the WPS handshake instead.

Figure 207 WPS: Example Network Step 3



Limitations of WPS

WPS has some limitations of which you should be aware.

- WPS works in Infrastructure networks only (where an AP and a wireless client communicate). It does not work in Ad-Hoc networks (where there is no AP).
- When you use WPS, it works between two devices only. You cannot enroll multiple devices simultaneously, you must enroll one after the other.

  For instance, if you have two enrollees and one registrar you must set up the first enrollee (by pressing the WPS button on the registrar and the first enrollee, for example), then check that it successfully enrolled, then set up the second device in the same way.
- WPS works only with other WPS-enabled devices. However, you can still add non-WPS devices to a network you already set up using WPS.

  WPS works by automatically issuing a randomly-generated WPA-PSK or WPA2-PSK pre-shared key from the registrar device to the enrollee devices. Whether the network uses WPA-PSK or WPA2-PSK depends on the device. You can check the configuration interface of the registrar device to discover the key the network is using (if the device supports this feature). Then, you can enter the key into the non-WPS device and join the network as normal (the non-WPS device must also support WPA-PSK or WPA2-PSK).
- When you use the PBC method, there is a short period (from the moment you press the button on one device to the moment you press the button on the other device) when any WPS-enabled device could join the network. This is because the registrar has no way of identifying the “correct” enrollee, and cannot differentiate between your enrollee and a rogue device. This is a possible way for a hacker to gain access to a network.

  You can easily check to see if this has happened. WPS works between only two devices simultaneously, so if another device has enrolled your device will be unable to enroll, and will not have access to the network. If this happens, open the access point’s configuration interface and look at the list of associated clients (usually displayed by MAC address). It does not matter if the

access point is the WPS registrar, the enrollee, or was not involved in the WPS handshake; a rogue device must still associate with the access point to gain access to the network. Check the MAC addresses of your wireless clients (usually printed on a label on the bottom of the device). If there is an unknown MAC address you can remove it or reset the AP.

E

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 106 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.

Table 106 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/ server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/ server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.

Table 106 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

F

Open Software Announcements

End-User License Agreement for “P-661HNU-Fx”

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED. HOWEVER, CERTAIN ZYXEL'S PRODUCTS MAY CONTAIN-IN PART-SOME THIRD PARTY'S FREE AND OPEN SOFTWARE PROGRAMS WHICH ALLOW YOU TO FREELY COPY, RUN, DISTRIBUTE, MODIFY AND IMPROVE THE SOFTWARE UNDER THE APPLICABLE TERMS OF SUCH THRID PARTY'S LICENSES ("OPEN-SOURCED COMPONENTS"). THE OPEN-SOURCED COMPONENTS ARE LISTED IN THE NOTICE OR APPENDIX BELOW. ZYXEL MAY HAVE DISTRIBUTED TO YOU HARDWARE AND/OR SOFTWARE, OR MADE AVAILABLE FOR ELECTRONIC DOWNLOADS THESE FREE SOFTWARE PROGRAMS OF THRID PARTIES AND YOU ARE LICENSED TO FREELY COPY, MODIFY AND REDISTIBUTE THAT SOFTWARE UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY. NONE OF THE STATEMENTS OR DOCUMENTATION FROM ZYXEL INCLUDING ANY RESTRICTIONS OR CONDITIONS STATED IN THIS END USER LICENSE AGREEMENT SHALL RESTRICT ANY RIGHTS AND LICENSES YOU MAY HAVE WITH RESPECT TO THE OPEN-SOURCED COMPONENTS UNDER THE APPLICABLE LICENSE TERMS OF SUCH THIRD PARTY.

1.Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2.Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3.Copyright

The Software and Documentation contain material that is protected by international copyright law, trade secret law, international treaty provisions, and the applicable national laws of each respective country. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4.Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, you may not market, co-brand, and private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the License Notice as below for the third party software, and your use of such material is exclusively governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software other than compliance with the applicable license terms of such third party, and makes no warranty (express, implied or statutory) whatsoever with respect thereto. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5.Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6.No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF

THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7.Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's TOTAL AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan if the parties agree to a binding arbitration. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License

Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

NOTE: Some components of this product incorporate free software programs covered under the open source code licenses which allows you to freely copy, modify and redistribute the software. For at least three (3) years from the date of distribution of the applicable product or software, we will give to anyone who contacts us at the ZyXEL Technical Support (support@zyxel.com.tw), for a charge of no more than our cost of physically performing source code distribution, a complete machine-readable copy of the complete corresponding source code for the version of the Programs that we distributed to you if we are in possession of such.

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes Bridge-utils, Busybox, Dnsmasq, Ebtables, Igmpproxy, Iproute2, Iptables, Linuxigd, Logrotate, MIPS linux kernel, Mtd-utils, Ntpclient, P910nd, Ppp, Samba, Syslog-ng, Sysstat, Updatedd, Strongswan, Wireless_tools, fuse, and Ntfs-3g under below GPL license

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose

authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code.(This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the

operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and

"any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes Dropbear and Ncurses under the MIT-Style License.

The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is

furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS ORIMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THEAUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHERLIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS INTHE SOFTWARE.

This Product includes libedit, Libpcap, Llbupnp, Openssh, Ppp, Pure-ftpd and Tcpdump under the license by BSD

BSD

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes Mini_httpd under the license by ACME Labs Freeware

ACME Labs Freeware License

All the free software available on the ACME Labs web site has a copyright notice like this one:

Copyright © 2000 by Jef Poskanzer <jef@mail.acme.com>. All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

1. Redistributions of source code must retain the above copyright
   notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
   notice, this list of conditions and the following disclaimer in the
   documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSEARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLEFOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIALDAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY

This Product includes Libbase64, Usbautomount and gmp under the LGPL License.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you.You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License").

Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you

accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be

distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCHDAMAGES.

END OF TERMS AND CONDITIONS.

This Product includes OpenSSL under the OpenSSL License.

OpenSSL Licens

```
/*
==========================================================================
=======
 * Copyright (c) 1998-2008 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
```

```
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 *
====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */
```

Original SSLeay License

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
```

* notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright

* notice, this list of conditions and the following disclaimer in the

* documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software

* must display the following acknowledgement:

* "This product includes cryptographic software written by

* Eric Young (eay@cryptsoft.com)"

* The word 'cryptographic' can be left out if the rouines from the library

* being used are not cryptographic related :-).

* 4. If you include any Windows specific code (or a derivative thereof) from

* the apps directory (application code) you must include an acknowledgement:

* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

*

* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND

* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

*

* The licence and distribution terms for any publically available version or

* derivative of this code cannot be changed. i.e. this code cannot simply be

* copied and put under another distribution licence

* [including the GNU Public Licence.]

*/

G

Legal Information

Copyright

Copyright © 2011 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the ZyXEL Device is subject to the terms and conditions of any related service providers.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1 Reorient or relocate the receiving antenna.

2 Increase the separation between the equipment and the receiver.

3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4 Consult the dealer or an experienced radio/TV technician for help.



FCC Radiation Exposure Statement

- Simultaneous transmission by using the 3g dongle is intended for this device.
- IEEE 802.11b or 802.11g or 802.11n(20MHz) operation of this product in the U.S.A. is firmware-limited to channels 1 through 11. IEEE 802.11n(40MHz) operation of this product in the U.S.A. is firmware-limited to channels 3 through 9.
- To comply with FCC RF exposure compliance requirements, (1) this device must be installed for use with both antennas providing a minimum separation distance of 20 cm from users and nearby persons, and (2) this device must also maintain 20 cm or more from other transmitters to prevent simultaneous transmission with nearby devices.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz and/or 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

Ce produit est conçu pour les bandes de fréquences 2,4 GHz et/ou 5 GHz conformément à la législation Européenne. En France métropolitaine, suivant les décisions n°03-908 et 03-909 de l'ARCEP, la puissance d'émission ne devra pas dépasser 10 mW (10 dB) dans le cadre d'une installation WiFi en extérieur pour les fréquences comprises entre 2454 MHz et 2483,5 MHz.

Viewing Certifications

1 Go to http://www.zyxel.com.

2 Select your product on the ZyXEL home page to go to that product's page.

3 Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the

warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index

A

AAL5 258
activation
  SIP ALG 179
  SSID 114
  wireless LAN
    scheduling 118
adding a printer example 61
administrator password 27
Advanced Encryption Standard, see AES
AES 319
AH 213
algorithms 213
alternative subnet mask notation 265
antenna
  directional 323
  gain 323
  omni-directional 323
AP (Access Point) 313
applications
  Internet access 21
Asynchronous Transfer Mode 244
ATM
  MBS 91, 94, 97, 100
  PCR 91, 94, 97, 100
  SCR 91, 94, 97, 100
ATM Adaptation Layer 5, see AAL5
audience 3
authentication 119, 121
  RADIUS server 121
automatic logout 28

B

backup
  configuration 239
bandwidth management 165
Basic Service Set, see BSS
Broadband 87
broadcast 103
BSS 122, 311
  example 122

C

CA 193, 318
CBR (Constant Bit Rate) 91, 94, 97, 100
certificate
  factory default 196
Certificate Authority, see CA
certificates 193
  CA 193
  replacing 196
  storage space 196
  thumbprint algorithms 195
  thumbprints 195
  trusted CAs 197, 198
  verifying fingerprints 195
Certification Authority, see CA
certifications 357
  notices 358
  viewing 358
channel 313
  interference 313
channel scan 108
channel, wireless LAN 106
client list 136
configuration 144
  backup 239
  reset 240
  restoring 240
copyright 357
CoS 174
CTS (Clear to Send) 314
CTS threshold 119

D

data fragment threshold 119
default LAN IP address 27
Denial of Service, see DoS
DH 219
DHCP 85, 132, 144, 145, 183
diagnostic 243
Differentiated Services, see DiffServ
Diffie-Hellman key groups 219
DiffServ (Differentiated Services)
  marking rule 174
disclaimer 357
DNS 132, 161
DNS Server
  for VPN host 217
DNS server address assignment 104
domain name system, see DNS
Domain Name System. See DNS.
DS (Differentiated Services) 174
DS field 174
DSCP 174
DSL line, reinitialize 245
dynamic DNS 183
Dynamic Host Configuration Protocol, see DHCP
dynamic secure gateway address 204
dynamic WEP key exchange 318
DYNDNS wildcard 183

E

EAP Authentication 317
Encapsulation 100
  MER 100
  PPP over Ethernet 100
encapsulation 87, 215
  RFC 1483 101
encryption 121, 319
ESP 213
ESS 312
Extended Service Set IDentification 108, 115
Extended Service Set, see ESS
external antenna 258

F

File Sharing 138
file sharing 22
filters
  MAC address 120
firewalls 185
  configuration 187
  security 188
firmware 237
fragmentation threshold 119, 314
frequency range 259
FTP 176

H

hidden node 313
host 227
host name 85
humidity 256

I

IANA 145, 146, 270
IBSS 311
ID type and content 218
IEEE 802.11g 315
IEEE 802.11g wireless LAN 258
IEEE 802.11i 258
IGMP 103
  version 103
IGMP proxy 258
IGMP v1 258
IGMP v2 258
IKE phases 216
importing trusted CAs 198
Independent Basic Service Set, see IBSS
initialization vector (IV) 320
inside header 215
install UPnP 148
  Windows Me 148
  Windows XP 149

intended audience 3
Internet access 21
Internet Assigned Numbers Authority
  See IANA
Internet Assigned Numbers Authority, see IANA
Internet Key Exchange 216
Internet Protocol Security, see IPSec
Internet Service Provider, see ISP
IP address 85, 145
  default 27
  ping 243
  WAN 88
IP Address Assignment 103
IP multicasting 258
IP pool 135
IP pool setup 145
IPSec 203
  algorithms 213
  architecture 212
  NAT 213
  see also VPN
ISP 87
ITU-T G.992.1 245

L

LAN 131
  and USB printer 143
  client list 136
  MAC address 137
LAN TCP/IP 145
limitations
  wireless LAN 122
  WPS 128
Local Area Network, see LAN
login
  passwords 27
logout 28
  automatic 28
logs 223, 235

M

MAC 85, 191
MAC address 137
  filter 120
MAC address filtering 191
MAC filter 191
managing the device
  good habits 25
  using FTP. See FTP.
Maximum Burst Size (MBS) 102
Maximum Burst Size, see MBS
Maximum Transmission Unit, see MTU
MBS 91, 94, 97, 100
MBSSID 122
Media access control 191
Media Access Control, see MAC Address
Message Integrity Check, see MIC
MIC 319
model name 85
MTU 92, 95, 98
MTU (Multi-Tenant Unit) 103
multicast 103
Multiple BSS, see MBSSID
multiple PVC support 257
multiplexing 101
  LLC-based 101, 258
  VC-based 101, 258
multiprotocol encapsulation 101
my IP address 204

N

NAT 145, 176, 270
  definitions 180
  how it works 180
  IPSec 213
  SIP ALG 179
    activation 179
  traversal 214
  what it does 180
negotiation mode 217
Network Address Translation, see NAT
network map 30

O

operation humidity 256
operation temperature 256
outside header 215

P

Pairwise Master Key (PMK) 320, 321
passphrase 110
passwords 27
PBC 123
PCR 91, 94, 97, 100
Peak Cell Rate (PCR) 102
Peak Cell Rate, see PCR
PHB 174
PIN, WPS 123
  example 125
power adaptor 259
power specifications 256
PPP over Ethernet, see PPPoE
PPPoE 87, 101, 257
  Benefits 101
preamble 119
preamble mode 315
pre-shared key 219
print server 22
Printer Server 143
printer sharing
  and LAN 143
  configuration 56
  requirements 143
  TCP/IP port 56
product registration 359
protocol 87
PSK 320
Push Button Configuration, see PBC
push button, WPS 123

Q

QoS 165, 174
Quality of Service, see QoS
Quick Start Guide 27

R

RADIUS 316
  message types 317
  messages 317
  shared secret key 317
RADIUS server 121
registration
  product 359
reinitialize the ADSL line 245
related documentation 3
Request To Send, see RTS
reset 240
RESET button 25
restart 241
restoring configuration 240
RFC 1483 101
RFC 1631 175
RFC 2516 257
RIP 95
router features 21
Routing Information Protocol, see RIP
RTS (Request To Send) 314
  threshold 313, 314
RTS threshold 119

S

safety warnings 7
scan 108
scheduling
  wireless LAN 118
SCR 91, 94, 97, 100
secure gateway address 204
security
  wireless LAN 119
security associations, see VPN
security, network 188
service access control 229

Service Set 37, 108, 115
Service Set IDentification 37
SIP ALG 179
  activation 179
SSID 37, 120
  activation 114
  MBSSID 122
stateful inspection 257
static route 157
status 83
storage humidity 256
storage temperature 256
subnet 263
subnet mask 145, 264
subnetting 266
Sustain Cell Rate, see SCR
Sustained Cell Rate (SCR) 102
syntax conventions 5
system
  firmware 237
  passwords 27
  status 83
System Info 84
system name 85, 232

T

TCP/IP port 56
temperature 256
Temporal Key Integrity Protocol, see TKIP
The 88
thresholds
  data fragment 119
  RTS/CTS 119
TKIP 319
traffic shaping 101
trusted CAs, and certificates 197
tunnel mode 215
tutorial
  wireless 44

U

unicast 103
Universal Plug and Play, see UPnP
upgrading firmware 237
UPnP 137
  forum 132
  security issues 132
USB features 22
USB printer 22

V

version
  firmware
    version 85
Virtual Circuit (VC) 101
Virtual Local Area Network See VLAN
Virtual Private Network, see VPN
VLAN 103
  Introduction 103
VPN 203
  established in two phases 203
  IPSec 203
  security associations (SA) 203
  see also IKE SA, IPSec SA

W

WAN
  MTU 92, 95, 98
  RIP 95
  Wide Area Network, see WAN 87
warnings 7
warranty 358
  note 359
Web Configurator 27
web configurator
  passwords 27
WEP 110, 121, 258
WEP Encryption 111
Wi-Fi Protected Access, see WPA
Wired Equivalent Privacy, see WEP

wireless
client configuration 46
security 315
tutorial 44
wireless client WPA supplicants 320
wireless LAN 105
authentication 119, 121
BSS 122
example 122
channel 106
encryption 121
example 105
fragmentation threshold 119
limitations 122
MAC address filter 120, 258
MBSSID 122
preamble 119
RADIUS server 121
RTS/CTS threshold 119
scheduling 118
security 119
SSID 120
activation 114
WEP 121
WPA 121
WPA-PSK 121
WPS 123, 125
example 126
limitations 128
PIN 123
push button 123
wireless network
example 105
wireless security 315
WLAN 105
auto-scan channel 108
interference 313
passphrase 110
scheduling 118
security parameters 322
see also wireless.
WEP 110
WLAN button 23
WPA 121, 258, 319
key caching 320
pre-authentication 320
user authentication 320
vs WPA-PSK 320
wireless client supplicant 320
with RADIUS application example 321
WPA2 319
user authentication 320
vs WPA2-PSK 320
wireless client supplicant 320
with RADIUS application example 321
WPA2-Pre-Shared Key, see WPA2-PSK
WPA2-PSK 319, 320
application example 321
WPA-PSK 121, 319, 320
application example 321
WPS 123, 125
example 126
limitations 128
PIN 123
example 125
push button 123